

جرائم المعلوماتية

الدكتور طارق الخن



Books

جرائم المعلوماتية

الدكتور طارق الخن

من منشورات الجامعة الافتراضية السورية

الجمهورية العربية السورية 2018

Cyber Crime

Tarek Al Khan

Publications of the Syrian Virtual University (SVU)

Syrian Arab Republic, 2018



الفهرس

الوحدة التعليمية الأولى: طبيعة شبكة الإنترنت والجرائم المرافقة لاستخدامها 1

الأهداف التعليمية 1

ماهية الإنترنت 2

التعريف بالانترنت 2

نشأة الانترنت 2

تعريف الانترنت 4

شبكة الانترنت والوب (w.w.w) 4

تنظيم الانترنت 5

بروتوكول تراسل الانترنت (TCP/IP) 5

الجهات المشرفة على الإنترنت 6

العناوين على شبكة الإنترنت والهيئات المانحة لها 7

القانون الجزائي والإنترنت 9

جرائم الإنترنت وجرائم المعلوماتية 9

التعريف بجرائم الإنترنت وجرائم المعلوماتية 9

الخصائص المتعلقة بجرائم الإنترنت 11

موقف الشريعة الإسلامية من جرائم الإنترنت 13

المواجهة التشريعية للجريمة المعلوماتية 13

المصطلحات التقنية المتعلقة بالجرائم المعلوماتية 19

الوحدة التعليمية الثانية:الجرائم المستحدثة 26

الاهداف التعليمية 26

الأحكام الموضوعية للجريمة المعلوماتية 27

الجرائم المستحدثة 28

صور الجرائم المستحدثة 29

جريمة الدخول غير المشروع إلى منظومة معلوماتية 29

جريمة شغل اسم موقع إلكتروني 35
جريمة إعاقة الوصول إلى الخدمة........ 38
جريمة إعتراض المعلومات........ 39
جريمة تصميم البرمجيات الخبيثة وإستخدامها 43
جريمة تصميم وترويج البرمجيات الخبيثة........ 44
جريمة إستخدام البرمجيات الخبيثة 46
جريمة البريد الواغل........ 48
الإحتيال عن طريق الشبكة 49
الإستعمال غير المشروع لبطاقات الدفع........ 56
جريمة الحصول دون وجه حق على بيانات أو أرقام بطاقات الدفع........ 62
جريمة تزويربطاقة الدفع........ 65
جريمة إستعمال بطاقة دفع مزورة أو مسروقة أو مفقودة 69
جريمة إنتهاك الحياة الخاصة........ 71
الأحكام العامة لجرائم المعلوماتية 73
ظروف التشديد........ 73
الشروع........ 75
العلنية على الشبكات المعلوماتية........ 76
المصادرة 77
الوحدة التعليمية الثالثة: الجرائم التقليدية........ 81
الأهداف التعليمية........ 81
الجرائم التقليدية والشبكة 82
تطبيق النصوص الجرائية 82
إرتكاب الجرائم التقليدية بإستخدام الشبكة أو عليها........ 82
إرتكاب الجريمة على جهاز حاسوبي أو منظومة معلوماتية بقصد التأثير على عملها أو على المعلومات المخزنة عليها........ 84
الأعمال الدعائية والتحريض على إرتكاب الجرائم........ 85

الوحدة التعليمية الرابعة: الإختصاص القضائي 89
الأهداف التعليمية 89
الاختصاص القضائي 91
الموقف القانوني والقضائي المقارن من مسألة الاختصاص 93
الاتفاقية الأوربية حول الجريمة الإفتراضية لعام 2001 93
القانون العربي الاسترشادي (النموذجي) لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها لعام 2004 94
الولايات المتحدة الأمريكية 95
بريطانيا 97
فرنسا 98
إيطاليا 98
الإمارات العربية المتحدة 99
مصر 99
مسألة الإختصاص في ظل التشريع السوري 100
الصلاحية الإقليمية 100
الصلاحية الذاتية أو العينية 103
الصلاحية الشخصية 104
الصلاحية الشاملة 105
الوحدة التعليمية الخامسة: الضابطة العدلية 109
الأهداف التعليمية 109
الأجهزة المختصة بمكافحة جرائم المعلوماتية 111
الأجهزة المختصة بمكافحة جرائم المعلوماتية على المستوى الوطني 111
الأجهزة المختصة بمكافحة جرائم المعلوماتية على المستوى الدولي و الأوربي 117
اختصاصات الضابطة العدلية في مكافحة جرائم المعلوماتية 120
تقديم الأخبار أو الشكوى عن جرائم المعلوماتية 121
استقصاء الجرائم وإثباتها 122

القبض 128
التفتيش 132
الضبط 137
الوحدة التعليمية السادسة: طرق الإثبات المستحدثة (الدليل الرقمي) 141
الأهداف التعليمية 141
ماهية الدليل الرقمي 143
تعريف الدليل الرقمي 143
مزايا الدليل الرقمي 143
مساوئ الدليل الرقمي 144
مصادر الدليل الرقمي ودور الإنترنت في التحقيقات الجرمية 145
حجية الدليل الرقمي 150
الولايات المتحدة الأمريكية 150
إنكلترا 153
فرنسا 153
المنظمة الدولية لدليل الحاسوب 154
سورية 155
المراجع 159

الوحدة التعليمية الأولى

طبيعة شبكة الإنترنت والجرائم المرافقة لاستخدامها

الكلمات المفتاحية:

التعريف بالإنترنت – تنظيم الإنترنت – جرائم الإنترنت – المصطلحات التقنية

الملخص:

تتضمن هذه الوحدة التعليمية التعرف على الإنترنت وتنظيمها وآلية عملها، والفرق مابين جرائم الإنترنت وجرائم المعلوماتية، والمصطلحات التقنية التي نص عليها قانون مكافحة الجريمة المعلوماتية في المادة الأولى منه.

الأهداف التعليمية:

تهدف هذه الوحدة التعليمية الى تعليم الطالب القدر الضروري من الأمور التقنية التي لا بد منها لفهم جرائم المعلوماتية، ومن هذه الأمور:

1. نشأة الإنترنت
2. برتوكول الإنترنت
3. الجهات المشرفة على الإنترنت
4. الفرق مابين جرائم المعلوماتية وجرائم الإنترنت
5. المصطلحات التقنية المتعلقة بجرائم المعلوماتية

إن معرفة ماهية شبكة الإنترنت، والفهم الجيد لآلية عمل هذه الشبكة، ثم التعرف على جرائم الإنترنت الناشئة عن الاستخدام السيئ لها، مسألة ضرورية للوقوف على مختلف أنواع الجرائم المعلوماتية. وبناءً على ذلك سوف نقسم هذا الجزء إلى:

أولاً– ماهية الإنترنت.

ثانياً – القانون الجزائي والإنترنت.

ماهية الإنترنت

يتطلب التعرف على ماهية شبكة الإنترنت، إلقاء الضوء على المراحل التي مرت بها هذه الشبكة منذ نشأتها. ثم معرفة آلية تنظيمها وكيفية عملها.

أ– التعريف بالإنترنت

إن الحديث عن الإنترنت يدفعنا للعودة إلى جذور هذه الشبكة منذ الستينيات؛ للتعرف على الأب الشرعي لها، ومتابعة مراحل نموها منذ الولادة، ثم استعراض التعريفات الفقهية التي تناولت شبكة الإنترنت، والتي تضمنت سمات هذه الشبكة.

أولاً– نشأة الإنترنت[(1)]:

نشأت فكرة الإنترنت نتيجة الحرب الباردة بين الولايات المتحدة الأميركية والاتحاد السوفييتي في الستينيات، حيث كان المسؤولون في وزارة الدفاع الأميركية يبحثون عن إجابة

---

(1) د.عبد الحسن الحسيني: القاموس الموسوعي في المعلومات والاتصالات والمعلوماتية القانونية، الطبعة الأولى، مكتبة صادر، بيروت، عام 2004، ص79–80.

- د.طوني ميشال عيسى: التنظيم القانوني لشبكة الإنترنت، الطبعة الأولى، منشورات صادر الحقوقية، بيروت، عام 2001، ص40.
- القاضي الدكتور إيهاب السنباطي: موسوعة الإطار القانوني للتجارة الإلكترونية، دار النهضة العربية، القاهرة، عام 2007، ص81.
- د.سليمان أحمد فضل: المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، عام 2007، ص4.
- د. عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، عام 2004، ص25.

لسؤال كان يتبادر إلى أذهانهم، **وهو كيف يمكن للمسؤولين في الولايات المتحدة الأميركية الاتصال فيما بينهم، في حال حدوث كوارث أو في حال حدوث هجوم نووي؟**

على إثر ذلك، عهدت وزارة الدفاع الأميركية في عام 1964 إلى وكالة مشاريع الأبحاث المتطورة (ARPA) [2] بمهمة إنشاء شبكة من الحواسيب تكون قادرة على الاستمرار في العمل في حال حدوث مثل هذه الكوارث.

في عام 1969، قامت وكالة مشاريع الأبحاث المتقدمة، بإنشاء شبكة متخصصة لهذا الغرض حملت اسم أربانت (ARPANET)، وكانت هذه الشبكة التجريبية في البداية تربط أربعة حواسيب آلية ضخمة فيما بينها.

في عام 1972، تمّ إيصال الأربانت إلى معظم الجامعات الأميركية، وفي عام 1973 بدأت الاتصالات الدولية بهذه الشبكة من إنكلترا و النروج. وهنا بدت الحاجة ملحة لإيجاد وسيلة تخاطب تسمح للحواسيب التي تعمل بلغات مختلفة بأن تتصل فيما بينها، فتمّ في هذا العام اكتشاف بروتوكول الإنترنت (TCP/IP)[3].

في عام 1986، تمّ نقل تشغيل أربانت من وزارة الدفاع إلى شبكة مؤسسة العلوم الوطنية NSFNET إضافةً إلى إدارة الطيران المدني والفضاء الأميركية، وكذلك إلى إدارة الطاقة، وبذلك أصبحت أربانت متاحة لجميع أشكال البحث العلمي.

في عام 1990، ومع انهيار الإتحاد السوفيتي وانتهاء الحرب الباردة، لم تعد تجد وزارة الدفاع الأمريكية أن هناك فائدة في حصر استعمال هذه الشبكة في الأمور العسكرية فقط، فأطلقت حرية استخدامها، وبدأ نطاق استعمالها يتسع، وأصبح لها إدارة خاصة لا ربحية، ثم تحولت أربانت إلى الإنترنت Internet كتسمية جديدة.

وفي عام 1991، تمكن مهندس الاتصالات الانكليزي "تيم بيرنرز لي" من اختراع تقنية

---

(2) وهو اختصار Agency Advanced Research Projects وهو مركز أبحاث عسكرية وعلمية تابع لوزارة الدفاع الأميركية.

(3) وهو بروتوكول تقني حول الاتصالات، يتضمن بروتوكولين مستقلين هما:

بروتوكول التحكم في النقل Transfer Control Protocol

وبروتوكول الإنترنت Internet Protocol

د.عبد الحسن الحسيني: المرجع السابق، ص792.

الوبّ[4] world wide web (w.w.w) التي تساعد على تصفح المعلومات واستعراضها بسهولة على شبكة الإنترنت.

ثانياً- تعريف الإنترنت:

تعددت المحاولات الفقهية لتعريف الإنترنت، ومن هذه التعاريف:

أن الإنترنت هي "عبارة عن آلية اتصال مكونة من مفاتيح وأسلاك وأماكن تخزين للبيانات، ودواعم توصيل، و روابط اتصال، تعمل في بوتقة واحدة بفضل بروتوكول الإنترنت (TCP/IP)"[5].

وفي تعريف آخر "بأنها شبكة الشبكات، حيث تتكون من عدد كبير من شبكات الحاسوب المترابطة والمتناثرة في أنحاء العالم، ويحكم ترابط تلك الأجهزة وتحادثها بروتوكول موحد يسمى بروتوكول تراسل الإنترنت"[6].

وهي أيضاً من وجهة نظر تقنية إنسانية، "بأنها تلك الوسيلة أو الأداة التواصلية بين شبكات المعلومات، دون اعتبار للحدود الدولية"[7].

والحقيقة إن جميع هذه التعاريف تعبر عن حقيقة الإنترنت، التي يمكن تعريفها ببساطة بأنها "**شبكة تتألف من عدد كبير من الحواسيب المتوضعة عبر العالم، والمترابطة مع بعضها البعض، والتي تستخدم في تواصلها بروتوكول تراسل الإنترنت**".

ثالثاً- شبكة الإنترنت والوبّ (w.w.w):

يظن الكثير من الناس بأن الإنترنت والوبّ w.w.w شيء واحد، غير أن ذلك ليس صحيحاً، لأن الإنترنت كما بيّنا هي عبارة عن شبكة تربط جميع شبكات الحاسوب المتصلة مع بعضها البعض. أما الوبّ w.w.w،

فهو أحد تطبيقاتها فقط، أو إحدى الآليات التي تستعمل في الاتصال.

---

(4) الوبّ web. هو نسيج العنكبوت.وقد سميت به هذه التقنية من باب المجاز. والوبّ هو الاسم المعرب لهذه التقنية، د.عبد الحسن الحسيني: المرجع السابق، ص860.

(5) القاضي الدكتور إيهاب السنباطي، المرجع السابق، ص78.

(6) د.عبد الفتاح مراد: شرح جرائم الكومبيوتر والإنترنت، بلا دار نشر، بلا عام، ص26.

(7) د.عمر بن يونس: المرجع السابق، ص38.

فالإنترنت تحتوي على عدة تطبيقات ووسائل للتواصل، مثل البريد الإلكترونيe-mail والماسنجر messenger والتي تستعمل في أفق الإنترنت، ولكنها ليست هي والإنترنت شيئاً واحداً. فالإنترنت تشبه الطريق التي تكون بين المدن، في حين أن تلك التطبيقات المذكورة وعلى رأسها الوبّ، هي أنواع وسائل المواصلات التي تستخدم هذه البنية الأساسية، مثل السيارات أو الحافلات أو الدراجات النارية[8].

وقد سبق وأشرنا بأن مهندس الاتصالات الإنكليزي "تيم بيرنز لي" هو من اخترع نظام الوبّ www، حيث يرتكز هذا النظام على بروتوكول (HTTP)[9] أي بروتوكول نقل النصوص الترابطية، الذي يسمح بربط مواقع الوبّ الموصولة بالشبكة فيما بينها والتجول فيها، وهو لا يعمل إلاّ بواسطة برامج تصفح خاصة[10].

ب- تنظيم الإنترنت

يتطلب التعرف على تنظيم الإنترنت، معرفة آلية عمل بروتوكول تراسل الإنترنت، ثم التعرف على الجهات التي تشرف على شبكة الإنترنت ودور هذه الجهات، خاصة الجهات المانحة للعناوين على الإنترنت، وهذا ما سنبحثه على التتالي:

أولاً- بروتوكول تراسل الإنترنت (TCP/IP)[11]:

تعتمد آلية عمل شبكة الإنترنت، على وسيلة التخاطب الرقمي، وذلك بواسطة بروتوكولين رئيسيين هما:

- بروتوكول التحكم في النقلTCP.
- برتوكول الإنترنت IP. ويسميان في التطبيق، بروتوكول تراسل الإنترنت

---

(8) القاضي الدكتور إيهاب السنباطي: المرجع السابق، ص80.

(9) وهو اختصار لـ Hypertext Transfer Protocol. د.عبد الحسن الحسيني:المرجع السابق،ص408.

(10) د.طوني عيسى: المرجع السابق، ص60.

(11) وهو بروتوكول تقني حول الاتصالات، يتضمن بروتوكولين مستقلين هما:

بروتوكول التحكم في النقل Transfer Control Protocol

وبروتوكول الإنترنت Internet Protocol

د.عبد الحسن الحسيني: المرجع السابق، ص792. القاضي الدكتور إيهاب السنباطي: المرجع السابق، ص79. د.طوني عيسى: المرجع السابق، ص44. د.محمد سعيد أحمد إسماعيل: أساليب الحماية القانونية لمعاملات التجارة الإلكترونية، رسالة دكتوراه مقدمة إلى جامعة عين شمس في القاهرة، عام 2005، ص37.

.TCP/IP

حيث يقوم بروتوكول التحكم في النقل TCP بتجزئة الرسالة المراد إرسالها إلى رزم من المعلومات، بحيث تحمل هذه الرزم معلومات تعريفية حول المرسل والمرسل إليه.

أما بروتوكول الإنترنت IP، فهو مسؤول عن عنونة وترقيم وتوجيه الرسائل إلى عناوينها المقصودة، كما يقوم بمنح كل جهاز أو موقع على الشبكة رقماً معيناً، قد يصل إلى 32 رقماً، حتى يتواصل مع بقية أطراف الشبكة. ونتيجة النمو المتزايد في المنظومات المتصلة بالشبكة، تمّ زيادة هذه الأرقام إلى 128 رقماً، وأي شبكة لا تستخدم هذين البروتوكولين لن تتمكن من الاتصال بالإنترنت.

بناء على ذلك، فإن الرسالة على الإنترنت تتحرك حاملة العنوان المقصود، وتنقسم إلى رزم قد ينطلق كل منها في اتجاه ومسار معين، فإذا وجدت إعاقة، سلكت طريقاً آخر. وتجري عند العنوان المقصود إعادة تكوين هذه الرسالة عن طريق تجميع الرزم المستلمة المكونة لها.

ثانياً- الجهات المشرفة على الإنترنت:

شبكة الإنترنت ليست ملكاً لأحد، ومن حيث المبدأ لا توجد هيئة رسمية وحيدة - حكومية أو غير حكومية- للإشراف على الإنترنت، ذلك لأن البنية الأساسية تدار بإشراف جهات غير حكومية، أخذت على عاتقها جعل الإنترنت مساحة حرة متاحة للجميع.

وتتصدر هذه الهيئات جمعية الإنترنت (Internet Society) ISOC، وهي مؤسسة أميركية أنشئت عام 1991، تهدف إلى تنسيق عمليات الاتصال والارتباط فيما بين الشبكات[12]. أما الجهات التي تقوم بإدارة البنية الأساسية للإنترنت فهي:

- الاتحاد الدولي للاتصالات ITU[13]، الذي يشرف على منظومات الاتصالات العالمية.
- منظمة الآيكان Icann[14]، وهي تشرف على أسماء المواقع وعناوينها (أسماء

(12) د:عبد الحسن الحسيني: المرجع السابق، ص 454. د.طوني عيسى: المرجع السابق، ص47.

(13) وهو اختصار لـ International Telecommunication Union د:عبد الحسن الحسيني: المرجع السابق، ص 456.

(14) وهو اختصار لـ .Internet Corporation For Assigned Name And Numbers د:عبد الحسن الحسيني: المرجع السابق، ص 414.

النطاقات).

ودون الدخول في الجدل حول مدى سيطرة هذه الجهات على الأركان الثلاثة للإنترنت (حواسيب، وكابلات اتصال، وأسماء النطاقات)، فإننا نكتفي بالقول بأنه: بدون هذه الأركان فلا حياة للإنترنت[15].

ثالثاً- العناوين على شبكة الإنترنت والهيئات المانحة لها:

لكي يتم تبادل ونقل البيانات والمعلومات عبر الإنترنت، يجب أن يكون لكل حاسوب أو نظام موصول بالشبكة عنوان خاص به وهو IP address، يسمح بالتعرف عليه وتعيين مركزه، كما هي الحاجة لمعرفة عنوان المرسل والمرسل إليه في البريد العادي.

وقد ذكرنا سابقاً بأن الإنترنت تمنح كل جهاز أو موقع على الشبكة عنواناً معيناً يصل إلى 32 رقماً وقد يصل إلى 128 رقماً، وبسبب طول هذه الأرقام، فإن مسألة تذكرها واسترجاعها أضحى أمراً عسيراً، لذلك فقد تمّ اختراع نظام أسماء النطاقات التي تعبر عن هذه الأرقام، فبدلاً من أن تدخل الرقم الطويل، يكفي أن تكتب مثلاً: www.tareq.com، و أن تنقر عليها نقرة واحدة، وبفضل نظام يعرف بـ http على الوبّ، سيتحول الاسم إلى العنوان الرقمي حتى يستكمل التواصل عبر الشبكة. وخلال هذه الرحلة يمر العنوان عبر مخدمات عملاقة[16]، مهمتها التعرف على هذه الأسماء وتمريرها.

ويمر أي اتصال في الشبكة بواحد من هذه المخدمات العملاقة (وتعدادها ثلاثة عشر على مستوى العالم)، فإن تعرفت عليه تواصل مع غيره، وإن لم تتعرف فلن يغادر الجهاز المرسل منه.

ويطلق على عنوان الإنترنتIP address، تسمية عنوان البريد الإلكتروني إذا كان يتعلق ببريد إلكتروني، ويسمى اسم النطاق إذا كان يختص بعنونة مواقع الوبّ.

وهناك معياران لتقسيم أسماء النطاقات، هما: المعيار الجغرافي، والمعيار النوعي.

---

(15) القاضي الدكتور إيهاب السنباطي: المرجع السابق، ص90.

(16) المخدّم server، هو عبارة عن حاسوب بمواصفات عالية، مزود بذاكرة كبيرة، وقنوات وأدوات اتصال. وفي حال وجود شبكة، فإن هذا الحاسوب يلعب دوراً رئيسياً، في مجال تقديم مختلف الخدمات للمستخدمين. د.عبد الحسن الحسيني: المرجع السابق، ص738.

فبالمعيار الجغرافي، تعطى كل دولة رمزاً من حرفين للدلالة عليها مثل sy. لسورية، و eg. لمصر، وuk. للملكة المتحدة، وfr. لفرنسا... وذلك باستثناء الولايات المتحدة الأميركية، حيث لا تحتاج مواقعها إلى تعريف جغرافي. وعلى ذلك فإن اسم أي نطاق لا يحمل تعريفاً جغرافياً سيكون حتماً مسجلاً في الولايات المتحدة الأميركية.

أما المعيار الثاني فهو يتعلق بنوع النشاط، ويضم تقسيمات سارية على مستوى العالم مثل edu. للجهات التعليمية، و gov. للجهات الحكومية، وcom. للجهات التجارية وغيرها، باستثناء اسم int. فهو محجوز للهيئات الدولية[17]. ولا بدّ من الإشارة إلى أن كل دولة موصولة بشبكة الإنترنت، تكون مسؤولة عن إدارة النطاق الخاص بها، كما يمكن أن تخلق نطاقات ثانوية ضمن نطاقها الأساسي، كأن تخلق مثلاً نطاقاً ثانوياً باسم gov، للدلالة على المواقع الحكومية في القطاع الأساسي sy. الذي يشير إلى الدولة السورية[18].

أما بالنسبة إلى الهيئات المانحة للعناوين على الشبكة، فهناك لجنة تسمى لجنة منح الأرقام على الإنترنت، وتعرف بـ IANA[19]، وهي تتولّى تنظيم عناوين المواقع في النطاقات التي ترمز إلى أسماء الدول، في حين أن صلاحية منح العناوين المستقلة يقع تحت إشراف الآيكان، وهي شركة أميركية خاصة لا تبتغي الربح تأسست في أيلول عام 1998، مركزها ولاية كاليفورنيا، وتتعامل مع العديد من الهيئات المتخصصة في عملية التسجيل الموزعة حول العالم[20].

(17) القاضي الدكتور إيهاب السنباطي: المرجع السابق، ص91-92.

(18) د.طوني عيسى: المرجع السابق، ص72.

(19) وهو اختصار لـ Internet Assigned Number Authority. د.عبد الحسن الحسيني: المرجع السابق، ص413.

(20) د.طوني عيسى: المرجع السابق، ص69.

القانون الجزائي والإنترنت

لما كانت جرائم الإنترنت من المواضيع الحديثة التي شغلت رجال القانون على اختلاف مشاربهم، الأمر الذي دفعهم للبحث في أغوارها بغية فهم طبيعتها. لذلك فقد كان من الواجب أن نخصص هذا الجزء لدراسة جرائم الإنترنت والتعرف على خصائصها لأنها تشكل القسم المتميز من جرائم المعلوماتية، ثم سنقوم بتسليط الضوء على المصطلحات التقنية التي نص عليها قانون مكافحة الجريمة المعلوماتية.

جرائم الإنترنت وجرائم المعلوماتية

تعدّ جريمة "دودة موريس" التي تعود واقعتها إلى 1988/11/2، هي الجريمة الأولى التي ارتكبت عبر الإنترنت حسب التاريخ القانوني، حيث استطاع الشاب "موريس" أن ينشر فيروس إلكتروني(21) تمكّن من مهاجمة آلاف الحواسيب عبر الإنترنت، وقد تسبّب بأضرار بالغة، أبرزها: توقف آلاف الأنظمة عن العمل، وتعطيل الخدمة... وقد قدرت الخسائر لإعادة إصلاح هذه الأنظمة وتشغيل المواقع المصابة بحوالي مائة مليون دولار (22).

ومنذ ذلك الحين ورجال القانون يبحثون عن تعريف لجرائم الإنترنت لفهم طبيعتها وخصائصها ومعرفة مكانتها من جرائم المعلوماتية. كما أن رجال الفقه الإسلامي لم يقفوا مكتوفي الأيدي أمام هذه الظاهرة الإجرامية، بل على العكس قدموا الدراسات التي تبين موقف الشريعة الإسلامية من هذه الجرائم، كما واجه المشرعون على مختلف مشاربهم الجريمة المعلوماتية على المستوى الوطني والإقليمي. وهذا ما سنبحثه في هذا المطلب على التتالي:

<u>أولاً- التعريف بجرائم الإنترنت و جرائم المعلوماتية:</u>

تعددت محاولات الفقهاء في تعريف جرائم الإنترنت، ومنها:

- هي "ذلك النوع من الجرائم التي تتطلب إلماماً خاصاً بتقنيات الحاسب الآلي ونظم

(21) الفيروس: هو عبارة عن برنامج صغير يؤدي إلى تدمير الملفات المعلوماتية وأنظمة التخزين من أقراص مغناطيسية وغير ذلك. ويمكن أن ينتج الفيروس عن خطأ ما في البرمجة، كما يمكن أن يكون صادراً عن مبرمجين محترفين يبغون إلحاق الضرر بالآخرين. د.عبد الحسن الحسيني: المرجع السابق، ص 851.

(22) د.علي جبار الحسيناوي: جرائم الحاسوب والإنترنت، الطبعة الأولى، دار اليازوري العلمية للنشر والتوزيع، عمان، 2009، ص10.

المعلومات، لارتكابها أو التحقيق فيها ومقاضاة فاعليها[23]".

– أنها "الجرائم التي لا تعرف الحدود الجغرافية، والتي يتم ارتكابها بأداة هي الحاسب الآلي عن طريق شبكة الإنترنت، وبواسطة شخص على دراية فائقة[24]".

– وفي تعريف آخر "كل اعتداء يقع على نظم الحاسب الآلي وشبكاته أو بواسطتها[25]".

– كما أنها "الجرائم الناشئة عن استعمال التواصل بين الشبكات[26]".

– وهي أيضاً "تلك الجرائم العابرة للحدود والتي تقع على شبكة الإنترنت أو بواسطتها من قبل شخص على دراية فائقة بها[27]".

ونحن نؤيد هذا التعريف الأخير؛ لأنه يبرز خصائص جرائم الإنترنت. إلاّ أنه من الأفضل عدم تحديد هذه الجرائم بأنها عابرة للحدود، لأنها من الممكن أن تكون جرائم داخلية أو دولية أو ذات بعد دولي كما سنرى لاحقاً. لذلك نرى أن يكون تعريف جرائم الإنترنت بأنها: **تلك الجرائم التي تقع على شبكة الإنترنت أو بواسطتها من قبل شخص ذي معرفة تقنية.**

ولا بدّ هنا من التمييز بين جريمة الحاسوب وجريمة الإنترنت، **فجريمة الحاسوب** هي التي تُرتكب بواسطة الحاسوب أو على مكوناته المعنوية، فقد تُرتكب من خلال حاسوب واحد أو من خلال شبكة داخلية تضم عدة حواسيب دون أن يكون هناك ولوج إلى الإنترنت، كما هو الحال في الجرائم التي تهدف إلى سرقة معلومات الحاسوب أو إتلافها. أما **جرائم الإنترنت** فإن شرطها الأساسي هو اتصال الحاسوب بالإنترنت، فالحاسوب هو الوسيلة التي لا مفر منها للولوج إلى هذه الشبكة.

ولا بدّ من الإشارة هنا، إلى أن جانباً من الفقه– ونحن نؤيده– يستخدم مصطلح

---

(23) د.عبد الفتاح مراد: المرجع السابق، ص40.

(24) المحاميان منير وممدوح الجنبيهي: جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، عام 2005، ص13.

(25) المحامي محمد أمين الشوابكة: جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، عام 2006، ص10.

(26) د.عمر بن يونس :المرجع السابق، ص 71.

(27) نبيلة هبة هروال: الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، عام 2007، ص30.

الجريمة المعلوماتية أو الجريمة الإلكترونية، للدلالة على جرائم الحاسوب والإنترنت معاً، بحيث يشمل هذان المصطلحان كلا النوعين. ومن ثم فإن مصطلح الجريمة المعلوماتية أو الجريمة الإلكترونية، أكثر شمولاً من جريمة الإنترنت[28].

وقد عرف المشرع السوري الجريمة المعلوماتية في المادة الأولى من قانون مكافحة الجريمة المعلوماتية بأنها:(**جريمة تُرتكب باستخدام الأجهزة الحاسوبية أو الشبكة، أو تقع على المنظومات المعلوماتية أو الشبكة.)**

وبهذا يكون المشرع السوري قد أخذ بالرأي الفقهي المشار إليه، **واستخدم مصطلح الجريمة المعلوماتية** ليشمل هذا التعريف جرائم الإنترنت وجرائم الحاسوب في مصطلح جامع لهما.

<u>ثانياً– الخصائص المتعلقة بجرائم الإنترنت:</u>

تتميز جرائم الإنترنت بعدة خصائص تميزها عن جرائم الحاسوب وهي:

<u>أ–جرائم تُرتكب عبر شبكة الإنترنت أو عليها:</u>

إن اتساع حجم شبكة الإنترنت وسهولة الولوج إليها، والتزايد المستمر في استخدام هذه الشبكة، جعل منها مسرحاً لكثير من الأفعال الإجرامية. فمعظم الجرائم التقليدية أصبحت تُرتكب عبر الإنترنت كالتهديد بالقتل مثلاً، إضافة إلى أن هذه الشبكة لم تسلم بحد ذاتها من اعتداءات المجرمين التي تناولت أنظمتها ومعلوماتها كجريمة إعاقة خدمة الانترنت، واعتراض المعلومات المرسلة عبر الشبكة وغيرها.

<u>ب–مرتكب جرائم الإنترنت ذو معرفة تقنية:</u>

تعد المهارة التقنية المطلوبة لتنفيذ جرائم الإنترنت أبرز صفات مجرمي الإنترنت، فتنفيذ هذه الجرائم يتطلب قدراً من المهارات التقنية، سواء تم اكتسابها عن طريق الدراسة المتخصصة، أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات. إلا أن ذلك لا يعني ضرورة أن

---

(28) نبيلة هبة هروال: المرجع السابق، ص31 و 54. د.نائلة عادل محمد فريد قورة: جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، عام 2005، ص35. المحامي محمد أمين الشوابكة :المرجع السابق، ص10.

يكون مجرم الإنترنت على قدرٍ كبيرٍ من العلم في هذا المجال، فالواقع العملي أثبت أن أشهر مجرمي الإنترنت لم يحصلوا على مهاراتهم التقنية عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المضمار [(29)].

ج– الحاسوب هو أداة ارتكاب جرائم الإنترنت:

يعدّ الحاسوب وسيلة النفاذ إلى شبكة الإنترنت، ومن ثم لا يمكن تصور ارتكاب جريمة إنترنت من دونه، ولا عبرة هنا لشكل الحاسوب الذي قد يتخذ شكله التقليدي أو شكل الحاسوب الشخصي، أو قد يكون ضمن الهاتف النقال أو حتى ضمن ساعة اليد...الخ.

د– جريمة الإنترنت لا تعرف الحدود الجغرافية:

لا تعرف جريمة الإنترنت الحدود الجغرافية، أي أنها من الممكن أن تكون جريمة داخلية أو دولية أو ذات بعد دولي.

فهي جريمة **داخلية** عندما تقع كاملة في نطاق إقليم دولة معينة.

وجريمة **دولية** عندما تتعلق بالقانون الدولي، أي عندما يكون أحد أطرافها شخصاً دولياً، على نحو ما حدث في التجسس الذي قامت به الولايات المتحدة الأميركية، عندما انتهكت أنظمة أعدائها الحاسوبية، وذلك بواسطة أسلحة معلوماتية فتّاكة، أثناء القصف الجوي للحلف الأطلسي في كوسوفو [(30)].

وقد تكون جريمة **ذات بعد دولي**، إذا اتفق المجتمع الدولي– بمقتضى اتفاقية دولية– بأن جريمة معينة تشكّل عدواناً على كل دولة، أو عندما ترتكب الجريمة داخل دولة معينة إلاّ أنها تمتد خارج إقليم تلك الدولة مثل جريمة ترويج المخدرات عبر الإنترنت[(31)].

هـ– صعوبة اكتشاف وإثبات جرائم الإنترنت:

تتصف جرائم الإنترنت بأنها صعبة الاكتشاف، لأن الجاني من الممكن أن يستخدم اسماً مستعاراً، أو أن يرتكب جريمته من خلال إحدى مقاهي الإنترنت. إضافة إلى أنها صعبة الإثبات

---

(29) د.نائلة عادل محمد فريد قورة: المرجع السابق، ص57.

(30) د.عمر بن يونس: المرجع السابق، ص 195– 197.

(31) د.عمر بن يونس: المرجع السابق، ص195.

لأنها لا تترك أثراً مادياً، بسبب إمكانية حذف الآثار المعلوماتية المستخدمة في ارتكاب الجريمة خلال ثوان[32].

ثالثاً– موقف الشريعة الإسلامية من جرائم الإنترنت:

لا شكّ أن رجال الفقه الإسلامي معنيون بما يستجد في الحياة من ظواهر، خاصة إذا كانت هذه الظواهر تتصل بأفراد المجتمع اتصالاً وثيقاً، لأن الفقيه يجب أن لا يقبع خلف النص الفقهي، بل يجب عليه أن يضع أحكاماً تتماشى مع الوقائع المستحدثة التي لم يرد فيها نص من قرآن أو سنة. لذلك فقد وضع الفقهاء منذ زمن طويل قاعدة فقهية هي " تغير الأحكام بتغير الأعراف والعادات والأزمنة والأمكنة"[33].

و هناك من يرى من فقهاء الشريعة بأنه إذا كانت شبكة الإنترنت من النظم المستحدثة، فإن ذلك لا يعني أن الشريعة ترفضها، ما دام هناك فوائد تعود على البشرية بفضل استخدامها، فالعلم النافع أمر تحبذه الشريعة وتحثّ عليه، ولا يمكن هنا إعمال القاعدة الفقهية القائلة: "دفع المفاسد مقدم على جلب المصالح"، لأن لشبكة الإنترنت فوائد عظيمة، والمفسدة تأتي بالاستغلال السيئ لها. فشبكة الإنترنت نفع في ذاتها. ولو أنه تمّ الأخذ بقاعدة دفع المفاسد، لما أخذت الشريعة بأي تقنية علمية، لأنه ما من اكتشاف إلاّ وله أضرار مثلما له فوائد. وإذا كانت الأضرار تأتي من خلال استعمال الفرد للإنترنت استعمالاً سيئاً، فيجب أن يعاقب هذا الفرد إذا كان فعله يعد جريمة من الجرائم، إذ إن نظرية العقاب في الشريعة الإسلامية تمتاز بالمرونة، ذلك أن نظام التعزير يصلح لكل زمان ومكان، إذا لم يشكل الفعل جريمة حد أو قصاص[34].

رابعاً: المواجهة التشريعية للجريمة المعلوماتية:

مع التزايد المستمر للجريمة المعلوماتية، ذهبت أغلب الدول إلى تجريم هذه الجريمة المستحدثة ضمن إطار المواجهة التشريعية لمختلف أنواعها. أما الدول التي لم تتصدَ تشريعياً لهذه الجريمة، فقد ذهب القضاء فيها إلى التوسع في تفسير النصوص الجزائية التقليدية لتشمل هذا النوع من الإجرام، بالرغم من أن هذا التوسع لم يسلم من النقد الفقهي.

---

(32) د.سليمان أحمد فضل: المرجع السابق، ص21.

(33) د.الشحات إبراهيم محمد منصور: الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية، دار النهضة العربية، القاهرة، بلا عام، ص80.

(34) د.الشحات إبراهيم محمد منصور: المرجع السابق، ص80–81–82.

وقد ظهرت إلى جانب المواجهة التشريعية على الصعيد الوطني مواجهة تشريعية على المستوى الإقليمي من خلال الاتفاقيات المعقودة في هذا الإطار، وسنلقي الضوء على هاتين الصورتين للمواجهة التشريعية على التتالي:

أ- التشريعات على الصعيد الوطني:

كانت الدول المتقدمة سباقة إلى مواجهة جرائم المعلوماتية، سواء عن طريق سن التشريعات الجزائية الخاصة بهذه الجرائم، أو من خلال تعديل النصوص القائمة لتشمل هذا الإجرام المستحدث.

- **ففي الولايات المتحدة الأمريكية** يعد قانون "فلوريدا" لجرائم الحاسوب الصادر في عام 1978 أول قانون في الولايات المتحدة الأمريكية يخاطب الاحتيال والتطفل على الحاسوب، حيث يَعتبر هذا القانون أن كل دخول غير مخول إلى الحاسوب هو بمثابة جريمة، حتى ولو لم يكن هناك نية عدائية من هذا الدخول.(35)

أما على الصعيد الفيدرالي، فقد صدر في عام 1984 قانون الاحتيال وسوء استخدام الكمبيوتر (CFAA)(36)، وتم تعديله في الأعوام 1986- 1988- 1989- 1990- 1994، ثم تم تعديله أخيراً عام 2001 بمقتضى القانون الوطني المؤرخ في 2001/10/26 "The patriot act"، حيث تم إدراجه في القسم 1030 من الباب /18/ من القانون الفيدرالي للولايات المتحدة الأمريكية.(37)

- **وفي بريطانيا** قام المشرع بإصدار قانون إساءة استخدام الكمبيوتر CAA لعام 1990 "Computer abuse act". وقد تضمن القسم الأول من هذا

---

(35) Eoghn Casey, Digital Evidence and computer crime, second edition, Acadimic Press ,2004, chapter- 2, p-1

(36) وهو اختصار لـ Computer Fraud And Abuse Act.

(37) The USA Patriot act هو القانون الوطني الأمريكي الصادر في 2001/10/26، وقد تناول تعديل حوالي خمسة عشر قانوناً، نذكر منها:

The ECPA of 1986, 18 USC Sec. 2701&Sec.
The CFAA of 1984, 18 USC Sec. 1030.
The Federal Wiretap Act, 18 USC Sec. 2510&Sec.

Eoghn Casey :op-cit, Chapter- 2, p-18 وأيضا د.عمر بن يونس: الإجراءات الجنائية عبر الإنترنت في القانون الأميركي، الطبعة الأولى، بلا دار نشر، 2005، ص9. والقسم 18u.s.c.1030 متوفر على موقع القوانين الأميركية: www.lawsource.com

القانون تجريم الدخول غير المشروع إلى النظام المعلوماتي (القرصنة)، أما القسم الثاني فقد تضمن تجريم الدخول غير المشروع مع عنصر إضافي وهو النية لارتكاب أو تسهيل ارتكاب جرائم، أما القسم الثالث فقد تضمن تجريم أي تعديل لمحتوى الحاسوب.[38] كما أصدر المشرع البريطاني **قانون الاحتيال لعام 2006**[39]، حيث سمح بموجبه بأن يكون الخداع موجهاً إلى نظام معلوماتي أو آلة، فلم يعد يُشترط أن يكون الخداع موجهاً إلى إنسان[40].

- **وفي فرنسا** قام المشرع بإصدار القانون رقم 19 لعام 1988، المتعلق بحماية نظم المعالجة الآلية للبيانات، ثم تم إدراج هذا القانون في قانون العقوبات الفرنسي لعام 1992 والذي طبق في 1994/3/1. [41]

فقد نصت المواد من 1-323 حتى 7-323 من قانون العقوبات على تجريم الدخول بشكل احتيالي أو البقاء غير المشروع في نظام المعالجة الآلية للبيانات أو في جزء منه. وتشدد العقوبة لهذه الجريمة إذا أدى الدخول غير المشروع إلى محو أو تعديل البيانات. كما جرمت هذه المواد تعطيل أو التدخل في عمل نظام المعالجة الآلية للبيانات. إضافةً إلى تجريم إتلاف أو تعديل البيانات في نظام المعالجة الآلي. كما عاقبت المادة 7-323على الشروع في ارتكاب هذه الجرائم، كما جرم القانون المذكور العديد من الجرائم.

وهناك العديد من الدول الأجنبية التي سنت تشريعات لمواجهة جرائم المعلوماتية مثل

---

(38) Robin Bryant, Investigating Digital Crime, John Wile& Sons،p:37-38
وأيضاً: القاضي الدكتور غسان رباح: الوجيز في قضايا حماية الملكية الفكرية والفنية مع دراسة مقارنة حول جرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، عام 2008، ص151.

(39) Fraud Act 2006، دخل هذا القانون حيز التنفيذ في كانون الثاني لعام 2007 وهو متوفر على موقع القوانين البريطانية: www.britishlaw.org.uk
.Robin Bryant, op- cit, p-42

(40) الفقرة الخامسة من المادة الثانية من هذا القانون.

(41) محمد عبيد الكعبي: الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، رسالة حاصلة على درجة الماجستير في القانون الجنائي بجامعة القاهرة، 2004. ص51. المحامي محمد أمين الشوابكة: المرجع السابق، ص23. د.أحمد حسام طه تمام: الجرائم الناشئة عن استخدام الحاسب الآلي، دراسة مقارنة، رسالة دكتوراه مقدمة لجامعة طنطا، 2000,المرجع السابق، ص350. ويوجد نسخة من قانون العقوبات الفرنسي لعام 1992 باللغة الإنكليزية على موقع القوانين الفرنسية على الإنترنت www.Legifrance.gouv.fr.

كندا وألمانيا وسويسرا وبلجيكا وغيرها[42].

كما أن المشرع العربي لم يقف مكتوف الأيدي أمام هذه الظاهرة، بل كانت هناك محاولات تشريعية في الدول العربية لاستيعاب هذا النوع من الإجرام، وقد قامت عدة دول عربية بمواجهة جرائم المعلوماتية وهي[43] :

- ففي **سلطنة عُمان** قام المشرع العماني بسن تشريع خاص لمكافحة جرائم المعلوماتية بموجب المرسوم السلطاني رقم 12 لعام 2011.
- **وفي الأردن** قام المشرع الأردني بإصدار قانون جرائم أنظمة المعلومات المؤقت رقم 30 لسنة 2010.
- وفي **المملكة العربية السعودية،** قام المشرع السعودي بإصدار نظام لمكافحة جرائم المعلوماتية في 31 آذار عام 2007.
- وفي **السودان،** فقد تم إصدار قانون جرائم المعلوماتية لعام 2007
- وفي **دولة الإمارات العربية المتحدة** فقد قامت بإصدار القانون الاتحادي رقم 2 لعام 2006 في شأن مكافحة جرائم تقنية المعلومات.
- **وفي قطر** قام المشرع القطري بتعديل قانون العقوبات رقم 11 لعام 2004، حيث تضمنت المواد (370 وحتى 387) جرائم الحاسب الآلي.

وقد جرمت معظم هذه القانونين العديد من جرائم المعلوماتية ومنها: الدخول غير المشروع إلى أنظمة الحاسوب، والالتقاط غير المشروع للمعلومات أو البيانات، وإتلاف أو محو البيانات والمعلومات، وتزوير بطاقات الائتمان واستعمالها وغير ذلك من الجرائم.

ب- الاتفاقيات على الصعيد الإقليمي:

هناك اتفاقيتين على الصعيد الإقليمي على قدر من الأهمية وهما: الاتفاقية الأوربية حول الجريمة الافتراضية، المعروفة باتفاقية "بودابست" لعام 2001. والاتفاقية العربية المتعلقة بالقانون العربي الاسترشادي (النموذجي) لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها لعام

(42) راجع في هذه التشريعات د.محمد طارق الخن، جريمة الاحتيال عبر الانترنت (الأحكام الموضوعية والأحكام الإجرائية)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت،2011،ص113 وما بعدها.

(43) جميع هذه التشريعات متوفرة على الإنترنت في عدة مواقع إلكترونية عن طريق محركات البحث.

.2004

- **فبالنسبة للاتفاقية الأوربية حول الجريمة الافتراضية (اتفاقية بودابست لعام 2001)**(44)، فقد قامت ست وعشرون دولة أوربية بالتوقيع على أول اتفاقية تكافح جرائم الإنترنت بتاريخ 2001/11/23 في بودابست "المجر"، كما قامت أربع دول من غير الأعضاء في المجلس الأوربي بالمشاركة في إعداد هذه الاتفاقية والتوقيع عليها أيضاً، وهي كندا واليابان وجنوب أفريقيا والولايات المتحدة الأمريكية.

وقد استغرقت المفاوضات بين الدول الموقعة على هذه الاتفاقية أربعة أعوام حتى تم التوصل إلى الصيغة النهائية المناسبة. ورغم أن هذه الاتفاقية هي في الأصل أوربية الميلاد، إلا أنها دولية الطابع، لأنها مفتوحة، أي تسمح بانضمام دول أخرى من غير المجموعة الأوربية، إلا أن هذه الدعوة للانضمام لا تسلخ عنها أنها اتفاقية تم إعدادها في إطار المجموعة الأوربية، وتتكون هذه الاتفاقية من 48 مادة موزعة على أربعة فصول غطت الجوانب الموضوعية والإجرائية للجريمة الافتراضية(45).

- **أما بالنسبة إلى القانون العربي الاسترشادي** فقد اعتمدت جامعة الدول العربية عبر الأمانة الفنية لمجلس وزراء العدل العرب ما سمي (**بقانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها)**، نسبة إلى مقدم هذا المقترح وهو دولة الإمارات العربية المتحدة. حيث تم اعتماده من قبل مجلس وزراء العدل العرب في دورته التاسعة عشرة بالقرار رقم (495- د19- 2003/10/8)، كما اعتمده مجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم (417، د2004/21)، ويتكون هذا القانون من 27 مادة تناولت الأحكام الموضوعية لجرائم المعلوماتية بصورة موفقة إلى حد ما، إلا أنه يؤخذ على هذا القانون الاسترشادي عدم تعرضه للأحكام الإجرائية الضرورية لملاحقة هذه الجرائم، فلم يتعرض لمسألة

---

(44) Europe Convention On Cyber-crime هذه الاتفاقية متوفرة على الموقع الإلكتروني conventions.co.int

(45) د. عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص216. د.سليمان أحمد فضل: المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، 2007، ص430 راجع في المراحل التي مرت بها الاتفاقية Allen Hammond, Santa Clara University, The 2001 Council Of Europe Convention On Cyber- Crime An efficient Tool To Fight Crime On Cyber- space, p- 42.

الاختصاص القضائي بشكل واضح، ولم يتضمن ما يشير إلى مدى إمكانية إخضاع البيانات أو المعلومات لإجراءات التفتيش والضبط، كما لم يتعرض إلى مفهوم الدليل الرقمي وشروطه وحجيته.

ومن الجدير بالذكر أنه تم إبرام **اتفاقية عربية جديدة لمكافحة جرائم تقنية المعلومات** بتاريخ 2010/12/21 بين الدول الأعضاء في جامعة الدول العربية، وقد تضمنت هذه الاتفاقية **إلزام** الدول الموقعة عليها بإصدار تشريعات داخلية تكافح جرائم المعلوماتية، وقد قامت سورية بالتوقيع على هذه الاتفاقية ممثلة بالسيد وزير الداخلية والسيد وزير العدل في القاهرة في التاريخ المذكور.

المصطلحات التقنية المتعلقة بالجرائم المعلوماتية

تستخدم التشريعات التي تكافح جرائم المعلوماتية مصطلحات تقنية في متن التشريع، وقد جرى العرف في صياغة مثل هذه التشريعات أن يلجأ المشرع إلى توضيح معاني هذه المصطلحات في مطلع التشريع، ولم يخرج المشرع السوري عن هذا المسار في قانون مكافحة الجريمة المعلوماتية، **فقد أوضح المشرع في المادة الأولى من قانون مكافحة الجريمة المعلوماتية** معاني المصطلحات المستخدمة في متنه، ثم جاءت التعليمات التنفيذية له لتزيد من هذا الإيضاح لفهم المقصود منها. والحقيقة أن هذه المصطلحات تعد بمثابة الأحرف الأبجدية المطلوبة لفهم هذا قانون، لذلك كان من الضروري الوقوف على معانيها قبل دراسة الجرائم التي نص عليها القانون.

وبناءً على ما تقدم سنبين معاني المصطلحات المتعلقة بدراستنا المنصوص عليها في المادة الأولى من قانون مكافحة الجريمة المعلوماتية فيما يلي[46]:

- **المعلومات:** (العلامات أو الإشارات أو النصوص أو الرسائل أو الأصوات أو الصور الثابتة أو المتحركة التي تحمل معنى قابلاً للإدراك، مرتبطاً بسياق محدَّد.)

وقد أعطى المشرع لمفهوم المعلومات معنى يتسع لمختلف أشكال هذه المعلومات وصورها، ويشترط في المعلومات أن يكون لها معنى قابل للإدراك ومرتبطة بسياق محدد، ولعل سبب إيراد هذا الشرط هو أن هناك من يميز بين المعلومات وبين البيانات، فالبيانات وفق هذا الرأي هي عبارة عن مجموعة من الكلمات والرموز والأرقام الخام التي لم تخضع للاستخدام والتي ليس لها معنى ظاهر يمكن إدراكه، أما المعلومات فهي المعنى الذي يمكن إدراكه من البيانات بعد معالجتها[47]، وفي تقديرنا أنه لا ضرورة إلى هذا التميز في دراستنا لأن البيانات هي المواد الخام للمعلومات القابلة للإدراك.

- **جهاز حاسوبي** computer device: (أي جهاز يستخدم التقانات الإلكترونية أو الكهرطيسية أو الضوئية أو الرقمية أو أي تقانات أخرى مشابهة بغرض توليد المعلومات

---

(46) جميع معاني المصطلحات المبينة تم إدراجها كما وردت في التعليمات التنفيذية الصادرة عن السيد وزير الاتصالات والتقانة بالقرار رقم 290 تاريخ 2012/5/7 مع إضافة بعض الإيضاحات الضرورية.

(47) راجع في هذا الرأي د.نائلة قورة، المرجع السابق، ص 97-98.

أو جمعها أو حفظها أو الوصول إليها أو معالجتها أو توجيهها أو تبادلها.)

ويشمل مفهوم الجهاز الحاسوبي على أي جهاز، سلكي أو لاسلكي، مهما كان نوعه أو شكله، يملك معالجاً للمعلومات، مثل المخدّم server والحاسوب الشخصي personal computer، والمساعد الرقمي الشخصي PDA، والهاتف الذكي smart phone، والمسيّر الشبكي router، الخ.

- **برمجيات حاسوبية** computer software: (سلسلة متّسقة من التعليمات المرمّزة التي يمكن تنفيذها على جهاز حاسوبي، بغية تمكينه من أداء الوظائف والتطبيقات المطلوبة.)

وقد تكون البرمجيات الحاسوبية مضمّنة في الجهاز الحاسوبي عند تصنيعه، وقد تكون أساسية كنظام التشغيل مثل نظام التشغيل windows أو تطبيقية يمكن تصميمها وتطويرها وتحميلها على الجهاز الحاسوبي كبرامج الألعاب، وبرامج تعليم اللغات، وبرامج المحاسبة التجارية، وبرامج الاتصالات مثل skype وغيرها من البرامج.

- **منظومة معلوماتية** information system: (مجموعة متّسقة من الأجهزة والبرمجيات الحاسوبية والمعدّات الملحقة بها.)

ومن الأمثلة على المنظومات المعلوماتية: جهاز حاسوبي مع برمجياته المضمّنة سواء كانت أساسية أو تطبيقية؛ أو مجموعة من الأجهزة الحاسوبية المترابطة في منظومة موزّعة distributed system؛ أو مخدّم تتصل به حواسيب طرفية؛ أو حاسوب مع المعدّات الملحقة به، كالمودم modem والطابعة والماسح الضوئي scanner؛ الخ.

- **الشبكة** network: (ترابط من الأجهزة الحاسوبية والمنظومات المعلوماتية يسمح بتبادل المعلومات أو التشارك فيها بين مرسِل ومستقبِل أو مجموعة من المستقبلين، وفق إجراءات محدَّدة.)

ومن الأمثلة على الشبكات: الإنترنت؛ وشبكات المعلومات الداخلية intranet؛ وشبكات تبادل المعطيات data communication network ؛ والشبكات النقّالة mobile network؛ والشبكات الهاتفية الذكية intelligent network؛ الخ.

- **موقع إلكتروني electronic site**: (منظومة معلوماتية، لها اسم أو عنوان يعرِّفها، وتتضمّن معلومات أو خدمات يمكن الوصول إليها عن طريق الشبكة، وبخاصة الإنترنت.)

من أهم الأمثلة على المواقع الإلكترونية: مواقع الوبّ website على الإنترنت مهما كان محتوها.

- **التواصل على الشبكة on-line communication**: (استخدام الشبكة، أو أي منظومة معلوماتية مشابهة، لوضع معلومات أو خدمات، ليس لها طابع المراسلات الشخصية، في متناول عامّة الجمهور أو فئة منه، بحيث يمكن لأي فرد الوصول إليها باتّباع إجراءات محدَّدة.)

ويقصد بالتواصل على الشبكة تقديم الخدمات التي يمكن للعموم public الوصول إليها؛ وهو يختلف عن المراسلات الشخصية بين مرسِل ومستقبِل محدَّد، واحد أو أكثر كالبريد الإلكتروني أو الرسائل النصّية القصيرة.

المحتوى content: (المعلومات أو الخدمات التي يمكن الوصول إليها وتداولها في إطار التواصل على الشبكة.)

من أصناف المحتوى الموضوع على الشبكة: المعلومات الموضوعة على المواقع الإلكترونية (المحتوى الإعلامي، النصّي والسمعي والبصري، والمحتوى الموسوعي، والمحتوى التجاري، الخ.)؛ والمعلومات المنشورة على المدوّنات blogs والصفحات الشخصية؛ والخدمات الإلكترونية (التجارة الإلكترونية، الحكومة الإلكترونية، الخ.) المقدَّمة على الإنترنت أو شبكات الهاتف، أياً كان نوعها (تسويق، بيع/شراء، معاملات، الخ.)؛ وخدمات التعليم عن بعد؛ الخ.

مقدِّم الخدمات على الشبكة on-line service provider: (أيٍ من مقدّمي الخدمات الذين يعملون في إطار التواصل على الشبكة؛ ومن أصنافهم: مقدّم خدمات النفاذ إلى الشبكة، ومقدّم خدمات التواصل على الشبكة، ومقدّم خدمات الاستضافة على الشبكة.)

- **مقدّم خدمات التواصل على الشبكة on-line communication provider**: (مقدّم الخدمات الذي يتيح التواصل على الشبكة، وذلك عن طريق موقع إلكتروني أو أكثر، أو

أي منظومة معلوماتية مشابهة.)

مقدّم خدمات التواصل على الشبكة يشمل كل من يقدّم معلومات أو خدمات على الشبكة، أياً كان نوعها، لعامة الجمهور أو فئة منه، على موقع إلكتروني أو أكثر، أو أي منظومة معلوماتية مشابهة، سواء أكان ذلك يتطلّب اشتراكاً أم لا يتطلّب، أو كان مجاناً أم في مقابل أجر، أو كان تفاعلياً أم لم يكن، ومن الأمثلة على ذلك مواقع التواصل الاجتماعي facebook وغيرها من المواقع.

- **مقدّم خدمات الاستضافة على الشبكة** on-line hosting provider: (مقدّم الخدمات الذي يوفّر، مباشرة أو عن طريق وسيط، البيئة والموارد المعلوماتية اللازمة لتخزين المحتوى، بغية وضع موقع إلكتروني على الشبكة؛ ويُسمّى اختصاراً المضيف host.)

مقدّم خدمات النفاذ إلى الشبكة on-line access provider: (مقدّم الخدمات الذي يتيح للمشتركين لديه النفاذ إلى الشبكة والوصول إلى المعلومات والخدمات المتوفّرة عليها.)

من أهم أشكال مقدّمي خدمات النفاذ إلى الشبكة: مقدّمو خدمات الإنترنت Internet service provider (ISP).

- **اسم موقع إلكتروني** electronic site name: (مجموعة من الرموز الأبجدية والرقمية، مخصّصة ومسجَّلة وفق قواعد محدَّدة، وتدلّ على موقع إلكتروني على الشبكة، وبخاصة الإنترنت، وتسمح بالوصول إليه.)

  والمثال على ذلك اسم موقع الجامعة الافتراضية السورية: www.svuonline.org

- **نطاق على الإنترنت** Internet domain: (زمرة من أسماء المواقع الإلكترونية على الإنترنت، تخضع لسلطة إدارية واحدة، وتندرج تحت اسم واحد هو اسم النطاق.)

  والمثال على ذلك نطاق مواقع الحكومة السورية والخاضع لإدارتها: syrgov.sy

اسم النطاق العُلوي top-level domain (TLD) name: (أوسع نطاق ينتمي إليه موقع إلكتروني ما على الإنترنت، ويُكوِّن الحقل الأخير من اسم هذا الموقع.)

و هذا هو المعيار النوعي لتقسيم النطاقات الذي سبقت الإشارة إليه ويكون في الحقل الأخير من اسم هذا الموقع ويرتبط بنوع النشاط، مثل edu. للجهات التعليمية، و gov. للجهات

الحكومية، و com. للجهات التجارية وغيرها

اسم النطاق العُلوي الوطني country-code top-level domain (ccTLD) name: (اسم نطاق عُلوي قياسي تندرج تحته جميع المواقع الإلكترونية أو موارد الإنترنت التي تديرها سلطة واحدة ذات صبغة وطنية.)

وهذا هو المعيار الجغرافي لتقسيم النطاقات المتبع عالمياً، والذي يعطى كل دولة رمزاً من حرفين للدلالة عليها مثل eg. لمصر، و uk. للملكة المتحدة، و fr. لفرنسا...

اسم النطاق العُلوي السوري: (اسم النطاق العُلوي الوطني للجمهورية العربية السورية؛ وهو ".سورية" و ".sy"، أو أي نطاق إضافي يُعتمد لاحقاً.)

بيانات الحركة traffic data: (أي معلومات يجري تداولها في إطار التواصل على الشبكة تحدّد، بوجه خاص، مصدر الاتصال ووجهته ومساره والمواقع الإلكترونية التي يجري الدخول إليها ووقت الاتصال ومدته.)

و تظهر أهمية بيانات الحركة في مجال التحقيق وإثبات جرائم المعلوماتية كمعرفة صاحب البريد الإلكتروني الذي أرسل الرسالة الإلكترونية المجرمة ووقت إرسالها ووصولها وغير ذلك من المعلومات.

ومن الجدير بالذكر أن هناك العديد من المصطلحات الأخرى التي أتى على ذكرها القانون لم تتم الإشارة إليها هنا تحاشياً للتكرار، لأننا سنتناولها بشكل تفصيلي فيما بعد، ولذلك اكتفينا فقط بتناول المصطلحات التي لا مفر من ذكرها قبل الغوص في جرائم المعلوماتية.

تمارين:

اختر الإجابة الصحيحة: جرائم المعلوماتية في الفقه الإسلامي هي من جرائم:

1. من جرائم الحدود
2. من جرائم القصاص والدية
3. من جرائم التعزير
4. جميع الإجابات السابقة خاطئة

الإجابة الصحيحة رقم 3

الأحكام الموضوعية

للجريمة المعلوماتية

الوحدة التعليمية الثانية

1- الجرائم المستحدثة

الكلمات المفتاحية:

جريمة الدخول غير المشروع إلى منظومة معلوماتية – جريمة شغل اسم موقع إلكتروني – جريمة إعاقة الوصول إلى الخدمة – جريمة اعتراض المعلومات – جريمة تصميم البرمجيات الخبيثة واستخدامها – جريمة إرسال البريد الواغل – جريمة الاحتيال عن طريق الشبكة – جريمة الاستعمال غير المشروع لبطاقات الدفع – جريمة انتهاك حرمة الحياة الخاصة - الأحكام العامة للجريمة المعلوماتية

المخلص:

تتضمن هذه الوحدة التعليمية شرح الجرائم المعلوماتية التي نص عليها المرسوم التشريعي 17 لعام2012، وهي تسعة صور من الجرائم، بالإضافة إلى شرح الاحكام العامة التي نص عليها قانون مكافحة الجريمة المعلوماتية.

الأهداف التعليمية:

تهدف هذه الوحدة التعليمية إلى تعريف الطالب على جرائم المعلوماتية وصورها التسعة المنصوص عليها بقانون مكافحة الجريمة المعلوماتية وهذه الجرائم هي:

1- جريمة الدخول غير المشروع إلى منظومة معلوماتية.
2- جريمة شغل اسم موقع إلكتروني.
3- جريمة إعاقة الوصول إلى الخدمة.
4- جريمة اعتراض المعلومات.
5- جريمة تصميم البرمجيات الخبيثة واستخدامها.
6- جريمة إرسال البريد الواغل.
7- جريمة الاحتيال عن طريق الشبكة.
8- جريمة الاستعمال غير المشروع لبطاقات الدفع.
9- جريمة انتهاك حرمة الحياة الخاصة.

ثم التعرف على الأحكام العامة المتعلقة بالجريمة المعلوماتية وهي: ظروف التشديد، والعلنية على الشبكة، والشروع، والمصادرة.

الأحكام الموضوعية للجريمة المعلوماتية

تقسم جرائم المعلوماتية إلى نوعين(1): **الأول: الجرائم التقليدية التي ترتكب بواسطة نظم المعلومات وخاصة شبكة الإنترنت**، وهي تلك الجرائم التي كانت موجودة قبل عصر المعلومات، ولكن بعد ظهور هذه التقنية وانتشار الشبكات أصبحت ترتكب بواسطتها، فراحت تبدو وكأنها جرائم جديدة. ومن هذه الجرائم: جريمة التهديد بالقتل وجريمتي الذم والقدح التي ترتكب عبر البريد الإلكتروني، والجرائم المخلّة بالأخلاق والآداب العامة التي ترتكب عبر المواقع الإباحية وغير ذلك من الجرائم.

أما **النوع الثاني: فهي الجرائم المستحدثة**، و يقصد بها تلك الجرائم التي ظهرت في عصر تقنية المعلومات ولم تكن معروفة من قبل وخاصة بعد اختراع الإنترنت، ومن أمثلة هذه الجرائم: جريمة الدخول غير المصرح به إلى أنظمة الحاسوب أو المواقع الإلكترونية، وجريمة تعطيل أو عرقلة نظام معلوماتي، وجريمة إتلاف المعلومات عن طريق زرع الفيروسات وغيرها من الجرائم.

و بناء على ذلك سندرس:

أولاً: الجرائم المستحدثة.

ثانياً: الجرائم التقليدية.

(1) د.حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت (دراسة مقارنة)، دار النهضة العربية- القاهرة،عام 2009، ص 79 و 217.

الجرائم المستحدثة

جرم المشرع السوري في الفصل الثالث من قانون مكافحة الجريمة المعلوماتية **تسع صور** مستحدثة لهذه الجريمة. كما نص المشرع في الفصل الخامس من قانون مكافحة الجريمة المعلوماتية على القواعد العامة التي تنطبق على الجرائم المنصوص عليها في هذا القانون، كظروف التشديد، وتجريم الشروع في الجنح، والعلنية على الشبكة وغير ذلك من القواعد.

وبناءً على ذلك سندرس:

- صور الجرائم المستحدثة.
- الأحكام العامة للجريمة المعلوماتية.

صور الجرائم المستحدثة

تضمن الفصل الثالث من قانون مكافحة الجريمة المعلوماتية النماذج القانونية لمختلف صور الجريمة المعلوماتية وهي:

1- جريمة الدخول غير المشروع إلى منظومة معلوماتية
2- جريمة شغل اسم موقع إلكتروني
3- جريمة إعاقة الوصول إلى الخدمة
4- جريمة اعتراض المعلومات
5- جريمة تصميم البرمجيات الخبيثة واستخدامها
6- جريمة إرسال البريد الواغل
7- جريمة الاحتيال عن طريق الشبكة
8- جريمة الاستعمال غير المشروع لبطاقات الدفع
9- جريمة انتهاك حرمة الحياة الخاصة

وسنتناول في هذا المطلب هذه الجرائم على التتالي:

أولاً- جريمة الدخول غير المشروع إلى منظومة معلوماتية:

تعد الحواسيب ومنظومات المعلوماتية والشبكات مستودعاً لكميات كبيرة من المعلومات، فإذا تم الوصول إلى هذه الأنظمة أمكن الوصول إلى هذه المعلومات المخزنة بها أو المتبادلة على اختلاف أشكالها، مثل أنظمة التشغيل والبرامج التطبيقية والملفات والبريد الإلكتروني وغيرها، وقد تعرضت الكثير من هذه الأنظمة الموجودة حول العالم إلى الدخول غير المشروع أو الاختراق من قبل أشخاص يعرفون بالقراصنة (Hackers)[(2)].

وعلى الرغم مما قد يترتب على الدخول غير المشروع إلى نظام الحاسوب من أضرار، فقد اتجه الكثيرين إلى المطالبة بضرورة تجريمه، إلا أن هناك رأياً يرى خلاف ذلك، ويستند هذا الرأي الأخير إلى أنه لا توجد ضرورة إلى تجريم الدخول غير المشروع إلى نظام الحاسوب كونه لم تبين الإحصائيات أن حجم هذه الجريمة قد وصل إلى ضرورة التدخل التشريعي، كما يرى أنصار هذا الرأي أن الدخول غير المشروع إلى نظام الحاسوب لا يحتاج إلى تجريم إذا لم يكن لدى صاحبه نية ارتكاب جريمة أخرى، فغالباً ما يكون هذا الدخول مجرد استعراض لبعض المهارات التقنية والفنية، وهذا لا يحتاج إلى تجريم، كما يذهب أنصار هذا الرأي إلى أن الدخول

---

(2) Hacker هو اسم للشخص الذي يدخل إلى نظام المعلومات أو قاعدة المعطيات أو إلى شبكة، دون أن يكون مسموحاً له بذلك. د.عبد الحسن الحسيني: المرجع السابق، ص 389.

غير المشروع الذي لا يخلف إتلافاً للمعلومات أو استخداماً لها لا يمكن الكشف عنه لأنه لا يترك أثراً مادياً يمكن أن يعتبر دليلاً في الإثبات، وأخيراً يرى أنصار هذا الرأي أن هناك صعوبة عملية ستواجه أجهزة التحقيق لما تتطلبه هذه الجريمة من ملكات فنية بالغة التعقيد، الأمر الذي سيقف حائلاً دون إسناد هذه الجريمة إلى مرتكبها.

وهناك من يرى – ونحن نؤيده– أن هذه الحجج لا تنال من ضرورة تجريم الدخول غير المشروع إلى أنظمة الحواسيب، ويرد أصحاب هذا الرأي على الحجج السابقة بأن الإحصائيات لا تبين الرقم الحقيقي لجريمة الدخول غير المشروع لأن هناك العديد من الحالات التي تقع فعلاً ولا يتم الإبلاغ عنها لأسباب مختلفة، وبالتالي لا تظهر هذه الإحصائيات الأرقام الحقيقية لهذه الجريمة، ويرد أنصار التجريم على الحجة الثانية بأن الدخول غير المشروع وإن لم يصاحبه نية ارتكاب جريمة لاحقه عليه، فإن هذه النية قد تتولد فيما بعد، ناهيك عن أن الدخول في حد ذاته ينطوي على المساس بسرية المعلومات، أما فيما يتعلق بصعوبة اكتشاف الدخول غير المشروع، فإن الواقع العملي يؤكد أنه قد تم بالفعل الكشف عن الكثير من حالات الاختراق إما عن طريق الإجراءات الأمنية التي يحتوي عليها نظام الحاسوب، وإما عن طريق الفاعل نفسه إذا أنه كثيراً ما يترك رسالة تشير إليه وذلك من قبيل التفاخر باختراقه، وأخيراً فيما يتعلق بالصعوبة الفنية التي تواجه التحقيق في هذه الجريمة، فإن هذه الصعوبة تواجه مختلف جرائم المعلوماتية بلا استثناء(3).

وقد قامت العديد من الدول بتجريم الدخول غير المشروع إلى أنظمة الحواسيب إلا أنها اختلفت في بعض الأحيان بالشروط المطلوبة لتطبيق هذه النصوص، فقد نص المشرع الفرنسي جريمة الدخول غير المشروع في المادة 323– 1 من قانون العقوبات الفرنسي، كما عاقب المشرع في بريطانيا على هذه الجريمة في المادة الأولى من قانون إساءة استخدام الحاسوب لعام 1990، وكذلك فعل المشرع الأمريكي في المادة 1030 (أ) من القانون الفيدرالي لجرائم الحاسوب، كما عاقبت المادة 2 من الاتفاقية الأوربية للجريمة الافتراضية لعام 2001 على جريمة الدخول غير المشروع إلى الحاسوب، وعاقبت أيضاً المادة الثانية من قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم 2 لعام 2006على هذه الجريمة، وهذا ما فعله أيضاً المشرع القطري في المادة 371 من قانون العقوبات رقم 11 لعام 2004، وهناك العديد من التشريعات الأجنبية والعربية والاتفاقيات التي عاقبت على جريمة الدخول غير المشروع إلى أنظمة المعلومات(4).

(3) راجع في أصحاب هذين الاتجاهين، د 0 نائلة قورة، المرجع السابق، ص 318 –319 0

(4) سبقت الإشارة في الفصل التمهيدي إلى المواقع الإلكترونية المتوفر عليها هذه القوانين.

- **وقد عاقب المشرع السوري على جريمة الدخول غير المشروع إلى منظومة معلوماتية في المادة 15 من قانون مكافحة الجريمة المعلوماتية** التي نصت على ما يلـي:

(أ- يُعاقَب بالغرامة من عشرين ألف إلى مئة ألف ليرة سورية، كل من دخل قصداً، بطريقة غير مشروعة، إلى جهاز حاسوبي أو منظومة معلوماتية أو موقع إلكتروني على الإنترنت، دون أن يكون له الحقّ أو يملك الصلاحية أو التصريح بالقيام بذلك.

ب- وتكون العقوبة الحبس من ثلاثة أشهر إلى سنتين والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية، إذا قام الفاعل بنسخ البيانات أو المعلومات أو التصاميم التي وصل إليها، أو إلغائها أو تغييرها أو تشويهها أو تزييفها أو استخدامها أو إفشائها.)

وعليه فسنتناول الركن المادي والركن المعنوي لهذه الجريمة ثم ننتقل إلى دراسة الظرف المشدد المنصوص عليه بالفقرة ب من هذه المادة.

<u>أ- الركن المادي</u>:

يتمثل النشاط الجرمي أو السلوك في جريمة الدخول غير المشروع إلى منظومة معلوماتية بفعل (الدخول)، **ويقصد بالدخول** هنا: جميع الأفعال التي تسمح بالولوج إلى نظام معلوماتي والوصول إلى المعلومات المخزنة به. وفعل الدخول يمكن أن **يتم <u>بطريقة مباشرة</u>** إلى الحاسوب أو منظومة معلوماتية، أي بالدخول كمستخدم دون أن يكون للفاعل الحق أو التصريح للقيام بذلك، كما يمكن أن يتم الدخول **<u>بطريقة غير مباشرة</u>** أي عن بعد عن طريق الشبكات كالإنترنت، وغالباً ما يتم الدخول بالطريقة المباشرة من قبل العاملين في الجهات المجني عليها، أما الطريقة غير المباشرة فيرتكبها أشخاص لا ينتمون إلى هذه الجهات[(5)].

ولم يشترط المشرع السوري في هذه الجريمة أن ينجح الفاعل في الوصول إلى المعلومات المخزنة، لأن نص التجريم يسمح بالعقاب بمجرد الولوج إلى نظام معلوماتي ولو لم يترتب على هذا الفعل أي ضرر أو فائدة، مادام الدخول كان بدون وجه حق، ويتحقق الولوج إلى النظام المعلوماتي بمجرد أن يبدأ الفاعل بتشغيل الحاسوب، لأن هذه الجريمة من الجرائم التي تمثل عدواناً محتملاً على الحق، وليست من الجرائم التي تتطلب العدوان على الحق الذي يحميه القانون[(6)].

وبناءً على ذلك فلا يعد دخولاً مجرد الإطلاع على المعلومات عن طريق قراءتها على شاشة الحاسب دون أن يقوم الفاعل قبل ذلك بأي عملية تقنية تسمح له بهذا الاطلاع، لأن

(5) د. نائلة قورة، المرجع السابق، ص 322.

(6) د. نائلة قورة، المرجع السابق، ص 343، د حسين الغافري، المرجع السابق، ص 39.

المشرع السوري قد اشترط صراحة في المادة 15 من قانون مكافحة الجريمة المعلوماتية أن يتم الوصول إلى المعلومات عن طريق فعل الدخول، فلا يكفي لتحقق النشاط الجرمي مجرد الإطلاع الذهني المحض على معلومات دون وجه حق ناهيك عن صعوبة إثبات مثل هذا الفعل.

ولا شك أن مجرد الدخول إلى الحاسوب أو منظومة معلوماتية أو موقع إلكتروني لا يشكل بحد ذاته جريمة، وإنما يستمد هذا الدخول عدم مشروعيته من كونه دون وجه حق أو دون صلاحية أو غير مصرح به.

ويقصد **بعدم مشروعية الدخول** هنا: انعدام سلطة الجاني في الدخول إلى النظام المعلوماتي مع علمه بذلك، وهذا يتطلب أساسا معرفة صاحب الحق في الدخول إلى هذا النظام، ويمكن القول أن الدخول إلى جهاز حاسوبي أو منظومة معلوماتية أو موقع إلكتروني يعد غير مشروع في الحالتين التاليتين:

الحالة الأولى: إذا كان دخول الفاعل إلى إحدى هذه الأنظمة المعلوماتية قد تم **دون الحصول على تصريح** من الشخص المسؤول عن النظام.

الحالة الثانية: إذا كان الفاعل مصرح له بالدخول إلى إحدى هذه الأنظمة ولكنه **تجاوز هذا التصريح الممنوح له** بالوصول إلى معلومات لا يشملها التصريح.

وغالباً ما يتم الدخول غير المصرح به في الحالة الأولى من قبل أشخاص خارج الجهات المجني عليها التي يوجد فيها النظام المعلوماتي المخترق، أما في الحالة الثانية فإن من يتجاوز التصريح الممنوح له بالوصول إلى معلومات هو غالباً شخص من داخل الجهة المجني عليها، ويصعب في هذه الحالة الأخيرة معرفة ما إذا كان العامل في هذه الجهة قد تجاوز بالفعل حدود اختصاصه، ولهذا ينبغي تحديد اختصاصات العاملين في مثل هذه الجهات تحديداً دقيقاً حتى يسهل تحديد التجاوزات في الصلاحية[7].

وتبدو أهمية التفرقة بين العاملين داخل الجهة التابع لها النظام المعلوماتي والخارجين عنها، في أن المشرع السوري قد شدد عقوبة الجريمة المعلوماتية في المادة 30 من قانون مكافحة الجريمة المعلوماتية إذا كان مرتكب الجريمة قد استغل عمله الوظيفي لارتكاب إحدى الجرائم المنصوص عليها في القانون المذكور.

أما النتيجة الجرمية في جريمة الدخول غير المشروع إلى منظومة معلوماتية فتبدو وكأنها مندمجة في النشاط الجرمي المتمثل بفعل (الدخول)، وقد أشرنا سابقاً بأن المشرع السوري

---

(7) د. نائلة قورة، المرجع السابق، ص 333

لم يشترط أن ينجح الفاعل في الوصول إلى المعلومات المخزنة لتحقق هذه الجريمة، وإنما يكفي أن يلج إلى النظام المعلوماتي، لأن علة التجريم تتمثل في حماية النظام ذاته من الدخول إليه دون وجه حق، وبناءً على ذلك يمكن تصور الشروع في ارتكاب جريمة الدخول غير المشروع عندما لا يتمكن الفاعل من الدخول إلى النظام المعلوماتي لظروف خارجه عن إرادته.

ب- الركن المعنوي:

جريمة الدخول غير المشروع إلى منظومة معلوماتية جريمة مقصودة، ويتمثل الركن المعنوي فيها بصورة القصد الجرمي العام بعنصريه العلم والإرادة.

وعليه يجب أن يتجه علم الجاني إلى أن فعله سيؤدي إلى الدخول إلى حاسوب أو منظومة معلوماتية أو موقع إلكتروني، ويجب أن يعلم فوق ذلك بأنه ليس له الحق أو الصلاحية في هذا الدخول.

كما يجب أن تتجه إرادته أيضاً إلى هذا الدخول غير المشروع، فإذا اعتقد الفاعل بناءً على أسباب معقولة بأن له الحق في الدخول إلى النظام المعلوماتي فإن القصد الجرمي لا يتوفر لديه. كما أنه لا يتوفر القصد الجرمي أيضاً إذا وجد الشخص نفسه داخل موقع إلكتروني عن طريق الخطأ أثناء تصفحه للإنترنت دون أن يكون مصرحاً له بالدخول إليه، ولكن يختلف الأمر إذا بقي هذا الشخص داخل الموقع الذي دخله خطأ إذا اتجهت إرادته إلى البقاء فيه مع علمه بأنه غير مصرح له بالدخول، ففي هذه الحالة يتوفر القصد الجرمي المطلوب لقيام هذه الجريمة.

جـ- العقوبـة:

عاقب المشرع على جريمة الدخول غير المشروع إلى منظومة معلوماتية بالغرامة من عشرين ألف ليرة إلى مئة ألف ليرة سورية، وهي عقوبة ذات وصف جنحوي لأنها تجاوزت ألفي ليرة سورية.

د- الظرف المشدد الخاص بجريمة الدخول غير المشروع إلى منظومـة معلوماتيـة:

شدد المشرع عقوبة جريمة الدخول غير المشروع إلى منظومة معلوماتية في الفقرة ب من المادة 15 من قانون مكافحة الجريمة المعلوماتية والتي نصت على ما يلي:

(ب - وتكون العقوبة الحبس من ثلاثة أشهر إلى سنتين والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية، إذا قام الفاعل بنسخ البيانات أو المعلومات أو التصاميم التي وصل إليها، أو إلغائها أو تغييرها أو تشويهها أو تزييفها أو استخدامها أو إفشائها).

حدد المشرع السوري الأفعال التي تعقب الدخول غير المشروع إلى منظومة معلوماتية

والتي تشكل ظرفاً مشدداً لهذه الجريمة و هي:

نسخ البيانات أو المعلومات أو التصاميم ويقصد **بالنسخ** أن يحصل الجاني على المعلومات أو التصاميم أو البرامج العائدة للمجني عليه مع بقاء النسخة الأصلية في حيازة هذا الأخير، وهذا ما يطلق عليه مصطلح سرقة المعلومات، مع أن معظم الفقه الجزائي _ وهو على حق _ يرى أن فعل الأخذ وهو جوهر النشاط الجرمي في جريمة السرقة يختلف عن النسخ، لأن هذا الأخير لا ينهي حيازة المجني عليه، وبالتالي لا تنطبق جريمة السرقة في مفهومها التقليدي على جريمة الحصول على المعلومات عن طريق نسخها بصورة غير مشروعة عملاً بمبدأ الشرعية الذي يستلزم عدم التوسع بتفسير النصوص الجزائية.[8]

أما **إلغاء المعلومات** فيقصد به حذفها أو محوها تماماً، أما **تغيير أو تشويه أو تزييف المعلومات** فيقصد به أي تعديل للمعلومات أو البرامج يقوم به الجاني والذي يمكن أن يؤدي إلى إتلاف هذه المعلومات أو عدم الاستفادة منها، أما **استخدام المعلومات** فيقصد به استعمالها بطريقة غير مشروعة، أما **إفشائها** فيصد به نشرها.

ولا بد من الإشارة هنا إلى أن المشرع السوري وأسوة بمعظم المشرعين قام بذكر مختلف الأفعال التي تقع على المعلومات دون وجه حق بقصد الإحاطة بها حتى لا يكون هناك أي فعل بمنأى عن العقاب[9].

أما **بالنسبة إلى الركن المعنوي** المطلوب لتطبيق ظرف التشديد المذكور، فلا بد من توفر القصد الخاص إلى جانب القصد العام الذي سبق وأن بيناه، **ويتمثل القصد الخاص** هنا أن يعلم الفاعل أنه يقوم بإحدى الأفعال الواردة بالفقرة ب من المادة 15، وأن تتجه إرادته إلى ارتكاب أحد هذه الأفعال.

ومن الأمثلة الشهيرة على جريمة الدخول غير المشروع إلى منظومة معلوماتية ونسخ ونشر المعلومات المخزنة بها، هو ما قام به القائمون على موقع ويكيليكس من عمليات اختراق إلى المواقع الإلكترونية لبعض الحكومات كالبيت الأبيض الأمريكي والبريد الإلكتروني للعديد من الجهات الحكومية ونشرها عبر الإنترنت من خلال موقع إلكتروني مخصص لهذه الغاية[10].

وفي قضية عرضت حديثاً على القضاء السوري، تتلخص بقيام موظف في إحدى

---

(8) راجع في هذا الموضوع د.عمر بن يونس، الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق، ص 402، د. هدى حامد قشقوس، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية – القاهرة، ص 70

(9) راجع التشريعات المتعلقة بمكافحة الجريمة المعلوماتية والتي سبقت الإشارة لها في الفصل التمهيدي.

(10) موقع ويكيليكس متوفر على العنوان www.wikileaks.org

شركات الهاتف النقال بنسخ أرقام هواتف مجموعة كبيرة من زبائن الشركة ومنها أرقام عائدة لجهات حكومية دون أن يكون مصرح له بذلك، ثم قام هذا الموظف بترك العمل من الشركة المذكورة، وقام بفتح شركة تجارية، وراح يستخدم هذه الأرقام من أجل تسويق بضائعه التجارية. وقد تم تحريك الدعوى العامة بحق الفاعل بجرم نسخ المعلومات دون وجه حق، وفق الفقرة ب من المادة 15 مع التشديد المنصوص بالمادة 30 من قانون مكافحة الجريمة المعلوماتية كونه موظفاً(11).

وفي قضية أخرى عرضت على قضائنا أيضاً، أنه في عام 2010 قام أحد الموظفين بعد تركه العمل في شركة تعمل في مجال المعلوماتية باختراق مخدم الشركة عبر الانترنت وإتلاف المعلومات المخزنة به، وقد قدر الضرر الذي لحق بهذه الشركة بحوالي ستة ملايين ليرة سورية. وقد حُركت الدعوى العامة بحق الفاعل بجرم الإضرار بأموال الغير وفق المادة 719 من قانون العقوبات(12).

وغني عن البيان بأن جريمة الدخول غير المشروع إلى منظومة معلوماتية بقصد الحصول على المعلومات أو تعديلها أو استخدامها قد تشكل حالة اجتماع جرائم مادي مع جريمة الاحتيال عبر الإنترنت، كما هو الحال عندما يتم الدخول بطريقة غير مشروعة إلى أحد المواقع الإلكترونية العائدة إلى مصرف ما بهدف التلاعب بالحسابات وتحويل الأموال من حساب المجني عليه إلى حساب الجاني.

ثانياً: جريمة شغل اسم موقع إلكتروني:

نصت المادة 16 من قانون الجريمة المعلوماتية على ما يلي:

(يُعاقَب بالحبس من شهر إلى ستة أشهر والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية، كل من شغل اسم موقع إلكتروني من دون علم صاحبه، أو حدّ من قدرة مالك نطاق على الإنترنت على التحكّم في هذا النطاق.)

و سنتناول الركن المادي والركن المعنوي لهذه الجريمة فيما يلي:

أ- الركن المادي:

يتمثل النشاط الجرمي في جريمة شغل اسم موقع إلكتروني من دون علم صاحبه **بانتحال**

(11) سجلات النيابة العامة بدمشق، رقم موجوداً 9286 / م تاريخ 9/19/ 2012م.

(12) ضبط فرع الأمن الجنائي بدمشق رقم 2719 تاريخ 7/5/ 2010 والدعوى مازالت منظورة أمام محكمة صلح الجزاء الثانية بدمشق برقم أساس 8 لعام 2012.

شخصية موقع إلكتروني، وهو شكل من أشكال سرقة الهوية على الإنترنت. و يتم هذا الأسلوب عن طريق إنشاء مواقع مزيفة على شبكة الإنترنت، على غرار مواقع الشركات والمؤسسات التجارية الأصلية الموجودة على هذه الشبكة، بحيث يبدو هذا الموقع المزيف وكأنه الموقع الأصلي المقدّم لتلك الخدمة. ويقوم الجناة عادة بالحصول على البيانات الخاصة بالموقع الأصلي وعنوانه ورقمه عن طريق الإنترنت، ثم يستخدمون هذه البيانات لإنشاء الموقع المزيف، بحيث يبدو للعيان شبيهاً بالموقع الأصلي، وبعد ذلك يقومون بتعديل البيانات السابقة على الموقع الأصلي، بحيث لا يكون على الإنترنت إلا موقع واحد بنفس العنوان. وهنا تظهر **النتيجة الجرمية** المتمثلة بالحد من قدرة صاحب الموقع من التحكم بموقعه. (13)

والمُشرع السوري لم يشترط لتحقيق جريمة شغل اسم موقع الكتروني أن يحصل الجاني على معلومات من المتعاملين مع هذا الموقع، بل تعتبر الجريمة قائمة متى استطاع الجاني شغل اسم هذا الموقع دون علم صاحبه أو الحد من قدرة مالكه من التحكم به. فهذه الجريمة تعتبر إحدى صور إعاقة الوصول إلى الخدمة أو الاستفادة منها، لأنها لا تهدف للحصول على المعلومات بصورة غير شرعية.

والحقيقة أن الحالات الواقعية والتطبيقات القضائية تشير إلى أن جريمة شغل اسم موقع إلكتروني غالباً ما ترتبط بجريمة الحصول على بيانات بطاقات الائتمان دون وجه حق. فبعد إنشاء الموقع المزيف، يستقبل الجناة عليه جميع المعاملات المالية والتجارية التي يقدمها عادة الموقع الأصلي لعملائه عبر شبكة الإنترنت، فيتم استقبال الرسائل الإلكترونية الخاصة بالموقع الأصلي والاطلاع عليها، ومن ثم يتم الاستيلاء على البيانات الخاصة بهم.

ففي إحدى القضايا، تم القبض في مصر على عصابة مكونة من ثلاثة أشخاص، لقيامهم بتصميم مواقع تشبه مواقع بعض المصارف، ثم قيامهم بإرسال رسائل عشوائية عن طريق البريد الإلكتروني إلى عملاء حقيقين، فينخدعون ويقومون بكتابة بياناتهم ويتبعون الخطوات التي يحددها لهم المتهمون. وبعد التعرف على البيانات السرية للعملاء، خاصة كلمات المرور السرية، يتم الاستيلاء على أرصدة هؤلاء الضحايا(14).

كما يمكن أن يتم انتحال الشخصية باستخدام بريد إلكتروني لخداع المتلقين، من أجل أن يتصلوا بمواقع إلكترونية مزيفة، وحملهم على إفشاء بياناتهم الشخصية والمالية، مثل أرقام

(13) د. جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، دار النهضة العربية، القاهرة، 2003، ص37.

(14) د. محمد الشناوي:جرائم النصب المستحدثة، دار الكتب القانونية، المحلة الكبرى، القاهرة، 2008، ص133.

بطاقات الائتمان وكلمات السر وأرقام الضمان الاجتماعي..[15]

والمثال على هذه العملية عندما يستلم أحد الأشخاص رسالة إلكترونية تتضمن طريقة اتصال بموقع إلكتروني (link)، فعندما ينقر المستلم على هذا الربط (link) فإنه يدخل إلى موقع مثل موقع e-bay، ولكن هذا الموقع يكون مزيفاً، إلا أنه وبالتفحص الجيد يمكن أن يظهر أن عنوان الصفحة مختلف عن الموقع الحقيقي. ولكن الضحية لن يلاحظ هذا الفرق، وسوف يقوم بإعطاء معلومات عنه، مثل كلمة السر وعنوان البريد.

ومن أمثلة هذا الأسلوب، أن شخصاً يدعى "ويليام جاكسون" استلم رسالةً إلكترونيةً تظهر أنها من موقع paypal، وهذه الرسالة تحذره بأن حسابه سوف يغلق ما لم يجدده بمعلومات مالية محددة، وكان يوجد في هذه الرسالة ربط (link) بالموقع الذي يستطيع من خلاله تجديد هذه المعلومات. وقد قام "جاكسون" بإدخال أرقام بطاقة الإئتمان والحسابات المصرفية وأرقام الضمان الاجتماعي الخاصة به، ومعلومات شخصية أخرى، وانتهت هذه العملية الاحتيالية بخسارة "جاكسون" مئات الدولارات[16].

كما تمّ تجريم الأخوين "ستيفينز" من "هيوستن" لقيامهما بتنصيب موقع إلكتروني مزيف لجيش الانقاذ Salvation Army، وقاما بجمع أكثر من 48000 دولار باسم جمعية إعصار كاترينا[17].

وفي قضية أخرى، ورد بلاغ إلى إدارة جرائم الحاسوب بوزارة الداخلية المصرية عبر البريد الإلكتروني، من إحدى شركات مكافحة جرائم الاحتيال العالمية، التي تمثّل قانوناً أحد البنوك البريطانية الكبرى، بوجود موقع مزيف على الإنترنت لهذا البنك البريطاني، يستخدم لخداع عملاء البنك وجمع المعلومات عنهم، والاستيلاء على أرصدتهم بطريقة احتيالية.

ونتيجة البحث والمتابعة، تم إلقاء القبض على طالب بكلية الهندسة مقيم بالإسماعيلية، لإنشائه هذا الموقع المزيف الذي يحمل نفس مواصفات الموقع الرئيسي للبنك، وقد استطاع الطالب خداع عملاء البنك في الخارج، كما استطاع بمعاونة أشخاص مقيمين في أوربا الشرقية وروسيا تحويل بعض أرصدة العملاء، عن طريق شركات تحويل الأموال وتقسيمها فيما بينهم، وقد ارتكب هذا الطالب جريمته عن طريق مقهى إنترنت عائد لوالده في الإسماعيلية[18].

---

(15) Micheal kunz and Patrick Wilson, computer crime and computer fraud ,University of Mayaland,2004, p-15.

(16) Micheal kunz and Patrick Wilson, op-cit, p- 16.

(17) IC3,Internet crime compliment center,2007, www.Ic3.gov , p-15.

(18) د. محمد الشناوي: المرجع السابق، ص97.

ولابد من الإشارة هنا إلى أن الجريمة شغل اسم موقع إلكتروني قد تشكل حالة اجتماع جرائم مادي مع عن جريمة الحصول دون وجه حق على بيانات بطاقات الدفع الإلكتروني باستخدام الأجهزة الحاسوبية أو الشبكة المنصوص عليها في المادة 22 من قانون مكافحة الجريمة المعلوماتية.

ب-الركن المعنوي:

جريمة شغل اسم موقع إلكتروني جريمة مقصودة، تتطلب القصد الجرمي العام بعنصريه العلم والإرادة، فيجب أن يعلم الجاني وأن تتجه إرادته إلى انتحال شخصية موقع إلكتروني دون علم صاحبه أو الحد من قدرة مالكه من التحكم به.

ج-العقوبة:

عاقب المشرع على جريمة شغل اسم موقع إلكتروني بعقوبة جنحوية الوصف وهي الحبس من شهر إلى ستة أشهر والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية.

ثالثاً-جريمة إعاقة الوصول إلى الخدمة:

نصت المادة 17 من قانون مكافحة الجريمة المعلوماتية على ما يلي:

(يُعاقَب بالحبس من ثلاثة أشهر إلى سنتين والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية، كل من أعاق أو منع قصداً، بأي وسيلة كانت، الدخول إلى منظومة معلوماتية أو الشبكة، أو عطّلها أو أوقفها عن العمل، أو أعاق أو منع قصداً، بأي وسيلة كانت، الوصول إلى الخدمات أو البرامج أو المواقع الإلكترونية أو مصادر البيانات أو المعلومات عليها.)

و سنتناول الركن المادي والركن المعنوي لهذه الجريمة.

أ- **الركن المادي:**

يتمثل النشاط الجرمي في جريمة إعاقة الوصول إلى الخدمة **بمنع الولوج** إلى منظومة معلوماتية أو إلى الشبكة كالإنترنت أو شبكة الهواتف النقالة، وقد تتخذ الإعاقة صورة تعطيل أو إيقاف الخدمة **كلياً** مثل وضع برمجيات تمنع المستخدم من الدخول إلى منظومة معلوماتية أو الإنترنت مطلقاً، أو قطع الاتصال كلياً، وقد يكون تعطيل الخدمة **جزئياً** كما هي الحالة عندما يتم منع أو حجب الوصول إلى أحد المواقع الإلكترونية، أو منع وصول رسائل البريد الإلكتروني إلى الجهة المقصودة.

ولم يشترط المشرع لارتكاب هذه الجريمة وسيلة معينة، فتتحقق هذه الجريمة مهما كانت

الوسيلة الإلكترونية المستخدمة، فقد تتم الإعاقة عن طريق إتلاف البرمجيات أو تعديلها أو إلغائها أو محوها، وهذا ما دفع البعض إلى اعتبار أن هناك تداخل بين جريمة إتلاف المعلومات وجريمة إعاقة الخدمة، فتعديل المعلومات أو إلغائها أو محوها يعد من وسائل إتلاف المعلومات كما يعد من وسائل إعاقة الوصول للخدمة. إلا أنه من الناحية العملية يمكن أن نميز بين هذين السلوكين، إذ أنه من الممكن أن يكون هناك إتلاف للمعلومات والبرامج دون أن يترتب على ذلك إعاقة الدخول إلى النظام، كما في حالة محو بعض الملفات التي يحتوي عليها النظام دون أن يؤثر ذلك على وظيفته، والعكس أيضاً صحيح. حيث يمكن أن يحدث إعاقة لنظام الحاسوب باستخدام وسيلة منطقية دون أن يترتب على ذلك إتلاف لأي من المعلومات أو البرامج التي يحتوي عليها، كما هو الحال عند إدخال برنامج يشكل عقبة تحول دون الدخول إلى النظام دون أن يؤدي ذلك إلى إتلاف أي من المكونات المنطقية للحاسوب[19]. ولعل هذا التميز ما دفع المشرع السوري إلى تجريم إعاقة الوصول للخدمة بنص خاص.

ولابد من الإشارة هنا أنه لا يدخل في تطبيق هذه المادة الحالات التي تكون بها إعاقة الخدمة ذات طابع مشروع، كحجب موقع إلكتروني تنفيذا لقرار قضائي أو تنفيذا للإجراءات التي تتخذها الهيئة الوطنية لخدمات الشبكة في الأحوال التي يخولها القانون ذلك.

ب- الركن المعنوي:

جريمة إعاقة الوصول إلى الخدمة جريمة مقصودة تتطلب توافر القصد الجرمي العام بعنصريه العلم والإرادة. فيجب أن يعلم الجاني بأنه يقوم بإحدى الأفعال الواردة بالمادة 17 التي من شأنها أن تؤدي إلى إعاقة الوصول إلى الخدمة، وأن تتجه إرادته إلى هذه الأفعال وإلى النتيجة الجرمية المتمثلة بحرمان المجني عليه من الدخول إلى منظومة معلوماتية أو إلى الشبكة. أما إذا تمت إعاقة الخدمة نتيجة خطأ الفاعل العرضي فينتفي القصد الجرمي وتنفي بذلك الجريمة برمتها.

ج-العقوبة:

عاقب المشرع على جريمة إعاقة الوصول إلى الخدمة بعقوبة جنحوية الوصف وهي الحبس من ثلاثة أشهر إلى سنتين والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية.

رابعاً: جريمة اعتراض المعلومات:

نصت المادة 18 من قانون مكافحة الجريمة المعلوماتية على ما يلي:

(19) د.نائلة قورة، المرجع السابق، ص 204. المحامي محمد أمين الشوابكة، المرجع السابق، ص223.

(أ– يُعاقَب بالحبس من ثلاثة أشهر إلى سنتين والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية، كل من اعترض أو التقط قصداً، بوجه غير مشروع، المعلومات المتداولة على منظومة معلوماتية أو الشبكة، أو تنصّت عليها.

ب– يُعاقَب بالحبس من شهر إلى ستة أشهر والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية، كل من استخدم الخداع للحصول على معلومات شخصية أو سرية من المستخدمين على منظومة معلوماتية أو الشبكة، يمكن استغلالها لأغراض إجرامية).

و سنتناول الركن المادي والركن المعنوي لجريمة اعتراض المعلومات ثم سنسلط الضوء على استخدام أسلوب الخداع للحصول على المعلومات.

أ– الركن المادي:

يتمثل النشاط الجرمي في هذه الجريمة بفعل الاعتراض على المعلومات بصورة غير مشروعة، **ويقصد بالاعتراض** أي عمل يهدف للوصول إلى المعلومات **المتداولة** على منظومة معلوماتية أو على الشبكة، بوسائل معلوماتية، **وذلك أثناء تبادلها**، سواء تم استخدام هذه المعلومات لاحقاً أم لا.

ولا يختلف مفهوم الالتقاط أو التنصت الوارد في متن المادة 18 عن مفهوم الاعتراض المتقدم مادام يؤدي إلى ذات النتيجة الجرمية أي الوصول إلى المعلومات **المتداولة** دون وجه حق، فلا تقوم هذه الجريمة إذا كان اعتراض المعلومات **مشروعاً** كقيام رجل الضابطة العدلية باعتراض المعلومات العائدة للمشتبه به بناءً على إذن من السلطة القضائية.

ويمكن تشبيه اعتراض المعلومات المتداولة على منظومة معلوماتية أو الشبكة بالتنصت على مكالمة هاتفية، فالهدف من الاعتراض هو معرفة محتوى الاتصال بين طرفين أو عدة أطراف، **أي أن الشرط الأساسي لقيام جريمة اعتراض المعلومات هو أن تكون المعلومات متداولة وليست مخزنة، أي التنصت على المعلومات أثناء عملية إرسالها أو استقبالها.**

ويتفق اعتراض المعلومات مع الدخول غير المشروع إلى منظومة معلوماتية، في أن كلاً منهما يؤدي إلى **نتيجة واحدة** وهي الوصول إلى معلومات غير مصرح للفاعل بالوصول إليها، فالفاعل في الحالتين أراد أن يصل إلى هذه المعلومات.

ولم يشترط المشرع وسيلة معينة لاعتراض المعلومات، فعالم تقنية المعلومات مليء بالبرامج التي تسمح بالتقاط أو اعتراض المعلومات، وهناك وسيلة تستخدم في هذا المجال تعرف بالتقاط الموجات الكهربائية وهي جمع للمعلومات عن بعد، فمن الممكن جمع معلومات يتم

إرسالها من أحد الحواسيب داخل مبنى، وذلك باستعمال شاشة عرض يتم توصيلها بجهاز تسجيل خارج المبنى، حيث يتم التقاط الموجات الكهربائية التي تحيط بالحاسوب ثم يتم تحويلها إلى معلومات مقروءة على الشاشة[20].

و يختلف اعتراض المعلومات عن الدخول غير المصرح به إلى منظومة معلوماتية، فإن هذه الجريمة الأخيرة يمكن أن تتم مباشرة أي عن طريق تشغيل الحاسب والوصول إلى المعلومات المخزنة دون وجه حق، ويمكن أن تتم بطريقة غير مباشرة أي عن بعد. أما اعتراض المعلومات فإن عملية تشغيل الحاسب تكون قد بدأت بالفعل بواسطة المجني عليه، ثم يأتي دور الجاني باعتراض أو التقاط أو التنصت على المعلومات المتبادلة.

ولقد أدى هذا الاختلاف بين الدخول غير المشروع إلى منظومة معلوماتية واعتراض المعلومات إلى الاتجاه نحو إفراد نص خاص يجرم اعتراض المعلومات، وقد أوصى المجلس الأوربي بضرورة إفراد نص خاص يجرم اعتراض المعلومات، وقد سارت عدة تشريعات على هذا النهج ومنها القانون البرتغالي حيث نص على جريمة اعتراض المعلومات في المادة الثامنة من القانون رقم 109 لعام 1991 الخاص بجرائم المعلوماتية[21].

<u>ب- الركن المعنوي:</u>

جريمة اعتراض المعلومات جريمة مقصودة، تتطلب القصد الجرمي العام بعنصريه العلم والإرادة، فيجب أن يعلم الفاعل أن ليس له الحق في اعتراض أو التقاط المعلومات أو التنصت عليها، ثم يجب أن تتجه إلى إرادته إلى اعتراض هذه المعلومات، ومتى توفر القصد الجرمي، فلا عبرة بعد ذلك للباعث أو الغاية من وراء التنصت على هذه المعلومات، فكون الدوافع نبيلة لا تؤثر على قيام القصد الجرمي، أما اعتراض المعلومات عن طريق الخطأ فلا تقوم به هذه الجريمة إلا إذا توفر القصد الجرمي بعد أن وجد الشخص نفسه يلتقط المعلومات المتبادلة ثم تولدت عنده عناصر القصد الجرمي أثناء التقاطه لهذه المعلومات دون وجه حق.

ج- <u>الحصول على معلومات بأسلوب الخداع:</u>

عاقب المشرع في فقرة ب من المادة 18 على استخدام الخداع للحصول على معلومات شخصية أو سرية من المستخدمين على منظومة معلوماتية أو الشبكة، يمكن استغلالها لأغراض إجرامية.

ويقصد بالخداع هنا الكذب الذي يتخذه الجاني حيال المجني عليه، لخلق اضطراب في

(20) د.نائلة قورة، المرجع السابق، ص350، د.حسين الغافري، المرجع السابق، ص374.

(21) د.نائلة قورة، المرجع السابق، ص351.

عقيدته وتفكيره بجعله يعتقد غير الحقيقة وحمله على تسليم الجاني معلوماته الشخصية أو السرية. وغالباً ما يتخذ أسلوب الخداع إحدى صورتين:

الصورة الأولى: إما إنشاء مواقع وهمية مشابهة للمواقع الأصلية العاملة على الإنترنت، حيث يظهر الموقع الوهمي بمظهر الموقع الحقيقي، وبالتالي يقوم المتعاملين مع هذا الموقع بالدخول إليه ووضع بياناتهم الشخصية أو السرية كالبيانات المتعلقة بحالتهم الصحية أو الاجتماعية أو المهنية أو التجارية وغيرها، وهنا يقوم الجاني بالحصول على هذه المعلومات.

أما **الصورة الثانية:** وهي خداع المجني عليه عن طريق البريد الإلكتروني، كقيام الجاني بإرسال رسالة إلكترونية إلى المجني عليه يعلمه بها بأن مصدر هذه الرسالة إحدى الجمعيات الاجتماعية التي تقدم الدعم المادي للعائلات، ويطلب من المجني عليه معلومات شخصية عنه، كالسن، وعدد أفراد الأسرة، والحالة الصحية والاجتماعية، والدخل الشهري، والمصارف التي يتعامل معها، وغير ذلك من المعلومات التي يمكن أن يستخدمها الجاني بارتكاب جريمة أخرى.

والحقيقة أن أسلوب الخداع المتبع للحصول على معلومات شخصية أو سرية غالباً ما يرتبط بجريمة الاستعمال غير المشروع لبطاقات الدفع، أي الحصول دون وجه حق على البيانات الخاصة ببطاقة الدفع الإلكتروني العائدة للمجني عليه، ثم قيام الجاني باستخدام هذه البيانات للاستيلاء على أموال المجني عليه. وتجب الإشارة هنا إلى أن المشرع السوري في قانون مكافحة الجريمة المعلوماتية أفرد نصاً خاصاً في المادة 22 يعاقب على الحصول دون وجه حق على بيانات بطاقات الدفع الإلكترونية، وفي هذه الحالة يطبق هذا النص الأخير لأنه هو النص الخاص حسب القواعد العامة[22].

ومن الأمثلة الشهيرة على الخداع عن طريق البريد الإلكتروني، رسالة تصل من شركة تطلق على نفسها اسم **E. A. A. S Lottery Watergate inc**، ومركزها "جوهانسبورغ"، وهي رسالة محترمة جداً، تظهر وكأنها صادرة فعلاً عن شركة تجارية، حيث تُعلمك بأنك ربحت 2.5 مليون دولار، وتطلبُ منك تأكيد نيتك باستلام المبلغ، كما تطلبُ منك المعلومات التالية:

1- الاسم الثلاثي.
2- عنوان المسكن.
3- رقم الهاتف.
4- رقم الفاكس.
5- صورة عن الهوية.

(22) المادة 180 من قانون العقوبات

وعندما ترسل هذه المعلومات، يرسلون إليك فاتورة باسمك تطالبك بمبلغ معين لقاء خدمات بريدية، وإذا أعطاهم الشخص المعني رقم حسابه أو رقم بطاقة الائتمان، فسوف يجد مفاجأة كبيرة في كشف المصرف آخر الشهر. والأكثر إثارة في هذا النوع من الرسائل هو مدى جديته، فقد طلبت إدارة هذه الشركة الوهمية من أحد الأشخاص ألا يرسل أي أوراق عبر البريد، وإنما يمكنه أن يحضرها بنفسه عند زيارته إلى مكاتب الشركة المنتشرة في 11 دولة بين آسيا وأوروبا والولايات المتحدة[23].

د- العقوبات:

عاقب المشرع بالفقرة أ من المادة 18 من قانون مكافحة الجريمة المعلوماتية على اعتراض المعلومات دون وجه حق بالحبس من ثلاثة أشهر إلى سنتين والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية، أما إذا تم الحصول على المعلومات عن طريق الخداع فتكون العقوبة أخف وهي الحبس من شهر إلى ستة أشهر والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية، ولعل سبب تشديد عقوبة اعتراض المعلومات أكثر من عقوبة الخداع بقصد الحصول على المعلومات، هو أن الجاني في جريمة اعتراض المعلومات يعبر عن خطورة إجرامية أكبر من استعماله الخداع، إذ أن اعتراض المعلومات يتطلب من الجاني قدرات تقنية أكبر من أجل التنصت على المعلومات أثناء تداولها، وهذا ما لا يحتاجه أسلوب الخداع الذي يكفي فيه في بعض الأحيان إرسال رسالة إلكترونية خادعة.

خامساً: جريمة تصميم البرمجيات الخبيثة واستخدامها:

نصت المادة 19 من قانون مكافحة الجريمة المعلوماتية على ما يلي:

(أ- يُعاقَب بالحبس من ثلاث إلى خمس سنوات والغرامة من خمسمئة ألف إلى مليونين ونصف مليون ليرة سورية، كل من يقوم بتصميم البرمجيات الخبيثة وترويجها لأغراض إجرامية.

ب-يُعاقَب بالحبس من ستة أشهر إلى ثلاث سنوات والغرامة من مئتي ألف إلى مليون ليرة سورية، كل من استخدم البرمجيات الخبيثة، أياً كان نوعها، وبأي وسيلة كانت، بقصد الإضرار بالأجهزة الحاسوبية أو المنظومات المعلوماتية أو الشبكة).

وبناءً على ذلك سنتناول جريمة تصميم البرمجيات الخبيثة المنصوص عليها في الفقرة أ من هذه المادة، وجريمة استخدام هذه البرمجيات الخبيثة المنصوص عليها في الفقرة ب.

(23) محمد عبيد الكعبي: الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، رسالة ماجستير مقدمة إلى جامعة القاهرة، عام 2004، ص176.

جريمة تصميم وترويج البرمجيات الخبيثة

وسنتناول الركن المادي والركن المعنوي لهذه الجريمة فيما يلي:

أ- <u>الركن المادي:</u>

عرف المشرع السوري البرمجيات الخبيثة في المادة الأولى من قانون مكافحة الجريمة المعلوماتية بأنها:" برمجيات حاسوبية مصمَّمة لإلحاق الضرر بالأجهزة الحاسوبية أو المنظومات المعلوماتية أو المواقع الإلكترونية أو الشبكة، أو تعطيل عملها أو تبطئته، أو تخريب محتوياتها أو مواردها، أو جمع معلومات عنها أو عن مالكيها أو مستخدميها أو عن بياناتهم دون إذنهم، أو إتاحة الدخول إليها أو استخدامها أو استخدام مواردها بصورة غير مشروعة ".

فالنشاط الجرمي يتمثل **بفعل التصميم والترويج** للبرمجيات الخبيثة،**ويقصد بالتصميم** القدرة على تخليق البرامج الخبيثة باستخدام إحدى لغات الحاسوب،أما **الترويج** فهو الإعلان عن هذه البرامج وإبراز مميزاتها وقدراتها التقنية. فلا يكفي لتحقق هذه الجريمة تصميم البرمجيات الخبيثة بل لا بد من أن يعقب عملية التصميم فعل الترويج المشار إليه، ويشترط أن يكون التصميم والترويج للبرمجيات الخبيثة لأغراض إجرامية مثل إتلاف معلومات الغير أو نسخ أو جمع هذه المعلومات.. الخ، ففي بعض الحالات يتم تصميم البرمجيات الخبيثة لأغراض مشروعة كحماية البرمجيات المؤجرة للغير التي لا يفقد مالكها حقوق الملكية عليها في الحالات التي يقوم بتأجيرها فقط، فإذا توقف المستأجر عن دفع بدل الإيجار، فإن ذلك يُعد إخلالاً بالالتزام التعاقدي، وغالباً ما يلجأ المالك هنا إلى وضع برمجية توقف عمل البرنامج المؤجر. مثلما حدث في برنامج طبي يقوم بتحليل وتشخيص الأمراض مثل مرض الشريان التاجي والسرطان.....الخ، حيث قامت الشركة المالكة له ببيع حق الانتفاع الايجاري لهذا البرنامج في عام 1995 لإحدى الشركات الطبية المُستخدمة له وهي شركة شمال تكساس للطب الوقائي، وتم تحميل هذا البرنامج على أجهزتها بعد أن دفعت ما قيمته 95% من قيمة العقد الذي لم يتضمن نقل الملكية الكاملة لهذا البرنامج. إلا أن شركة شمال تكساس لم ترتاح لهذا البرنامج بعد استخدامه، فطلبت من الشركة المالكة إلغاء العقد، وردت هذه الأخيرة برسالة تضمنت رفضها هذا الإلغاء وأنه سوف تقوم بإيقاف عمل البرنامج بتاريخ 1996/1/31 عن طريق قنبلة منطقية أو موقوتة. فقد تستخدم البرمجيات الخبيثة مثل القنابل الموقوتة أو المنطقية كبرنامج حماية للملكية الفكرية وذلك ضد النسخ عبر الإنترنت، فالذي يملك حقوق النسخ قد يُجيز للغير النسخ عبر الإنترنت إلا أن هذه الإجازة محدودة لفترة زمنية مُعينة تختفي بعدها البرمجية أو الملف المنسوخ بسبب القنبلة

الموقوتة[24].

ويمكن التميز بين فيروس الحاسوب وبين فيروس الإنترنت، ففي حالة فيروس الحاسوب فإن الفيروس يكمن بالحاسوب المُصاب به، ولا ينتقل إلى حاسوب آخر إلا بالعدوى عن طريق انتقال ملف أو برمجية من الحاسوب المُصاب إلى آخر غير مُصاب، أي لا بد هنا من التدخل الإنساني في عملية انتقال العدوى، أما في حالة فيروس الإنترنت فإن الفيروس يستمر بالانتشار إلى الحواسيب والشبكات دون الحاجة إلى تدخل إنساني سوى في أول مرة التي يتم بموجبها إرسال الفيروس عبر الإنترنت. الأمر الذي يجعل من فيروس الإنترنت أكثر انتشاراً وخطراً من فيروس الحاسوب[25].

وللبرمجيات الخبيثة أو الفيروسات أصناف عديدة ومن أكثر هذه الأصناف شيوعاً:

1- **حصان طروادة Trojan horse:** وهو عبارة عن **برمجية اختراق**، وهو صفة لنوعية من الملفات التي لديها القابلية للانتشار عن طريق نسخ ذاته إلى الملفات الأخرى والدخول إلى الأماكن السرية والمُشفرة فينتشر فيها ليحقق غرضه في التدمير والتخريب، وليس هناك نوعية واحدة لحصان طروادة إذ تندرج تحت هذه التسمية أنواع عديدة من الفيروسات[26].

2- **الدودة worm:** وهي عبارة عن برمجية تقوم بالانتقال من حاسوب إلى آخر دون حاجة إلى تدخل إنساني لتنشيطها، فهي تتمتع بخاصية التنشيط الذاتي وبهذا تختلف الدودة عن حصان طروادة.

ولقد ظهرت الدودة أول مرة في عام 1988 على يد طالب الدكتوراه في علوم الحاسوب بجامعة كورنل وهو Robert Tappan Morris، وقد عرفت بدودة موريس، التي تسببت في تدمير الآلاف من الحواسيب في الولايات المُتحدة الأمريكية، وتتسبب حركة الدودة في تعطيل الحاسوب بتجميد لوحة المفاتيح والشاشة والذاكرة وتبطئته. وهناك عدة أشكال من برامج الدودة الضارة ومن أشهرها دودة الحب و Anna Virus[27].

3- القنبلة المنطقية Logic bomb:

وهي عبارة عن برامج خبيثة يتم إدخالها بطرق غير مشروعة مع برامج أخرى، فهي من حيث الشكل ليست ملفاً مُتكاملاً وإنما شفرة تنضم إلى مجموعة ملفات البرامج وذلك بتقسيمها إلى

---

(24) د.عمر بن يونس، الجرائم الناشئة عن استخدام الإنترنت،ص 371- 372.

(25) د. عمر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، ص 365.

(26) د. عبد الحسن الحسيني، المرجع السابق، ص819 د. عمر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، ص366 د. حسين الغافري، المرجع السابق، ص 413.

(27) د. عبد الحسن الحسيني، المرجع السابق، ص87 1 د. عمر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، ص 367. د. حسين الغافري، المرجع السابق، ص 410.

أجزاء متفرقة هنا وهناك كي لا يتم التعرف عليها، بحيث تتجمع فيما بينها بحسب الأمر المُعطى لها في زمن معين أو عند حدوث واقعة معينة، ويؤدي اجتماعها هذا إلى انعدام القدرة على تشغيل البرامج الحاسوبية ونظام التشغيل في بعض الأحيان[28].

ب-الركن المعنوي:

جريمة تصميم وترويج البرمجيات الخبيثة جريمة مقصودة تتطلب القصد الجرمي العام بعنصريه العلم والإرادة كما يتطلب القصد الجرمي الخاص المُتمثل بنية التصميم والترويج لأغراض إجرامية.

فيجب أن يعلم الجاني بأنه يقوم بتصميم برمجيات خبيثة وأن تتجه إرادته إلى خلق مثل هذه البرمجيات، كما يجب أن يتجه العلم والإرادة لديه إلى ترويجها، ويجب أن تكون غايته من تصميم وترويج هذه البرمجيات أن تستخدم فيما بعد لأغراض إجرامية كإتلاف أو نسخ أو تعديل معلومات الغير وهنا يظهر الدافع أو القصد الخاص لهذه الجريمة، أما إذا قام شخص بتصميم وترويج برمجيات لغايات مشروعة كحماية حقوق الملكية الفكرية فلا يتوفر لديه القصد الجرمي وبالتالي فلا تقوم بحقه هذه الجريمة برمتها.

جريمـة استخدام البرمجيـات الخبيثـة

نصت الفقرة ب من المادة 19 من قانون الجريمة المعلوماتية على ما يلي:

(ب-يُعاقَب بالحبس من ستة أشهر إلى ثلاث سنوات والغرامة من مئتي ألف إلى مليون ليرة سورية، كل من استخدم البرمجيات الخبيثة، أياً كان نوعها، وبأي وسيلة كانت، بقصد الإضرار بالأجهزة الحاسوبية أو المنظومات المعلوماتية أو الشبكة).

وسنتناول الركن المادي والركن المعنوي لهذه الجريمة.

أ- الركن المادي:

يتمثل النشاط الجرمي في جريمة استخدام البرمجيات الخبيثة بفعل الاستخدام و يُقصد **بالاستخدام** هنا استعمال هذه البرمجيات أو تحميلها ونشرها على الشبكة. وتبرز خطورة نشر هذه البرمجيات في أن شخصية المجني عليه وعدد الضحايا غير محدد، فعملية النشر تتشابه مع إطلاق الرصاص جُزافاً على جمع من الناس. لذلك فلهذه الجريمة خطورة خاصة لا يمكن تحديد

---

(28) د. عبد الحسن الحسيني، المرجع السابق، ص 493 د. عمر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، ص 370 - 371. د. حسين الغافري، المرجع السابق، ص 415.

الضرر الناتج عنها، حتى لو افترضنا أن إرسال الفيروس قد استهدف حاسوب شخص محدد فبعد تحميل هذا البرنامج الخبيث على حاسوب المجني عليه سيتم انتشاره إلى الحواسيب الأخرى نتيجة قدرة الفيروس على نسخ نفسه والانتقال من حاسب إلى آخر.

ونشر الفيروسات قد يتم **بطريقة مباشرة** عن طريق تحميلها على حاسوب معين. أو **بطريقة غير مباشرة** عن طريق نشرها بشكل عشوائي عبر الإنترنت، كما لو قام شخص بوضع ملف وثائقي على الإنترنت وكان هذا الملف يحتوي على فيروس لإتلاف أو نسخ المعلومات، وفي كلا الحالتين سيتم انتقال الفيروس إلى عدد غير محدد من الأجهزة الحاسوبية.

ومن أشهر القضايا التي عُرضت على القضاء الأمريكي وتحديداً في ولاية تكساس، قضية بيرلسون الشهيرة، وتتلخص هذه القضية في أن بيرلسون كان يعمل موظف أمن في شركة سمسرة، حيث قام بوضع برمجية تحوي فيروس حصان طروادة في نظام الحاسوب بغرض تدمير بيانات عمولة المبيعات، ولقد أُدين بيرلسون وعوقب بسبعة أعوام تحت المُراقبة(29).

<u>ب–الركن المعنوي:</u>

جريمة استخدام البرمجيات الخبيثة جريمة مقصودة تتطلب القصد الجرمي العام بعنصريه العلم والإرادة بالإضافة إلى القصد الجرمي الخاص المُتمثل بقصد الاضرار بالأجهزة الحاسوبية أو المنظومة المعلوماتية أو الشبكة.

فيجب أن يعلم الجاني أنه يستخدم أو ينشر أو يبث برمجيات خبيثة، ويجب أن تتجه إرادته إلى هذا الاستخدام، كما يجب أن يتوفر لديه الدافع وهو الإضرار بالحواسيب أو المنظومات أو الشبكات العائدة للغير.

ج– <u>التمييز بين عقوبة جريمة تصميم البرمجيات الخبيثة واستخدامها:</u>

عاقب المشرع على جريمة تصميم وترويج البرمجيات الخبيثة بعقوبة الحبس من ثلاث إلى خمس سنوات والغرامة من خمسمئة ألف إلى مليونين ونصف مليون ليرة سورية. كما عاقب على جريمة استخدام البرمجيات الخبيثة بالحبس من ستة أشهر إلى ثلاث سنوات والغرامة من مئتي ألف إلى مليون ليرة سورية.

ولا بد من الإشارة هنا إلى أن من يقوم بتصميم وترويج البرمجيات الخبيثة ثم يقوم باستخدامها بقصد الإضرار بالحواسيب تتوفر لديه حالة اجتماع الجرائم المادي، أي يُسأل عن جريمتين وليس عن جريمة واحدة، ويمكن أن تُدغم العقوبتين وتنفذ الأشد أو تُجمعان حسب القواعد العامة.

---

(29) د. عمر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، ص 374.

سادساً: جريمة البريد الواغل:

نصت المادة 20 من قانون مكافحة الجريمة المعلوماتية على ما يلي:

(يُعاقَب بالغرامة من عشرين ألف إلى مئة ألف ليرة سورية، كل من يقوم بإرسال بريد واغل إلى الغير، إذا كان المتلقي لا يستطيع إيقاف وصوله إليه، أو كان إيقاف وصوله مرتبطاً بتحمّل المتلقي نفقة إضافية.)

وسنتناول فيما يلي الركن المادي والركن المعنوي لهذه الجريمة.

أ- الركن المادي:

عرف المُشرع في المادة الأولى من قانون مُكافحة الجريمة المعلوماتية **البريد الواغل** بأنه: (أي شكل من أشكال الرسائل، مهما كان محتواها، التي تُرسل عبر الشبكة إلى الغير، دون رغبة المُتلقي في وصولها إليه)

و الواغل في اللغة هو (الرجل الذي يدخل على القوم في طعامهم وشرابهم من غير أن يدعوه إليه)[30]، و الواغل كما جاء في التعليمات التنفيذية لقانون مكافحة الجريمة المعلوماتية هي ترجمة مُقترحة تعبر عن مصطلح spam أي البريد الإلكتروني غير المرغوب فيه.

ولم يشترط المشرع في البريد الواغل أن يحتوي معلومات معينة، فقد يكون محتواه إعلامي أو إعلاني عن البضائع التجارية وغير ذلك. ولكن **يشترط** لتحقق هذه الجريمة أن يكون المُتلقي أو المُرسل إليه غير قادر على إيقاف وصول الرسائل غير المرغوب فيها له، أو كان إيقاف وصولها مرتبط بتحمل المُتلقي نفقات إضافية على نفقات الاشتراك بخدمة البريد الإلكتروني.

وبناءً على ذلك فلا تقوم هذه الجريمة إذا كان المُرسل إليه يستطيع إيقاف تدفق البريد الواغل أو الغير مرغوب به ولم يقم بإيقافه دون ترتب نفقات إضافية عليه، كما لا تقوم هذه الجريمة بحق مُرسل رسالة إعلانية أو عدة رسائل دون أن تُشكل إزعاجاً للمُرسل إليه.

ولم يشترط المُشرع السوري أن يؤدي البريد الواغل أو غير المرغوب فيه إلى تضخيم البريد الإلكتروني كما فعل المُشرع المقارن، فالمُشرع الولائي الأمريكي مثلاً يشترط أن يؤدي البريد غير المرغوب فيه إلى تضخم البريد الإلكتروني أي إغراق حساب البريد الإلكتروني عن طريق إرسال كمية كبيرة من الرسائل الإلكترونية مهما كان محتواها إلى صندوق بريد المُرسل إليه المُراد تعطيله، بحيث إذا امتلأ لم يعد بالإمكان فتحه أو التعامل معه كونه محدود المساحة، وهذا ما اشترطه المُشرع الأمريكي في ولاية واشنطن وولاية فيرجينيا وغيرها من الولايات[31]. فالمُشرع السوري لم يشترط تضخم البريد الإلكتروني إلى نحو يجعل من فتحه مُستحيلاً لأن هذه

---

(30) ابن منظور، مُعجم لسان العرب، مادة وغل.

(31) د. عمر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، ص 353- 354.

الحالة تعد جريمة من جرائم إعاقة الوصول إلى الخدمة المنصوص عليها في المادة 17 من قانون مكافحة الجريمة المعلوماتية.

ب-الـركن المعنـوي:

جريمة إرسال البريد الواغل جريمة مقصودة تتطلب القصد الجرمي العام بعنصريه العلم والإرادة.

فيجب أن يعلم الجاني بأنه يُرسل رسائل غير مرغوب فيها إلى المُرسل إليه ويجب أن تتجه إرادته إلى ذلك أيضاً، وبالتالي فلا تسأل مثلاً شركة للمواد الطبية عن إرسال عدة رسائل عن طريق الخطأ إلى أشخاص لا علاقة لهم بمهنة الطب، ثم توقفت الشركة عن إرسال هذه الرسائل الإعلانية عندما تبين لها الأمر.

جـ-العقـويـة:

عاقب المُشرع على جريمة إرسال البريد الواغل بالغرامة من عشرين ألف إلى مئة ألف ليرة سورية، وهذه الغرامة ذات وصف جنحوي لأنها تزيد عن ألفي ليرة سورية.

سابعاً: الاحتيال عن طريق الشبكة:

نصت المادة 21 من قانون مكافحة الجريمة المعلوماتية على ما يلي:

(أ-يُعاقَب بالحبس من ثلاث إلى خمس سنوات والغرامة من خمسمئة ألف إلى مليونين ونصف مليون ليرة سورية، كل من استولى، باستخدام الأجهزة الحاسوبية أو الشبكة، على مال منقول أو عقار، أو معلومات أو برامج ذات قيمة مالية، أو سند يتضمّن تعهداً أو إبراء أو أي امتياز مالي آخر، وذلك عن طريق خداع المجني عليه أو خداع منظومة معلوماتية خاضعة لسيطرة المجني عليه، بأي وسيلة كانت.

ب وتكون العقوبة الاعتقال المؤقّت، والغرامة من خمسمئة ألف إلى مليونين ونصف مليون ليرة سورية، في الحالات التالية:

1) إذا وقعت الجريمة على ثلاثة أشخاص فأكثر.

2) إذا تجاوز مبلغ الضرر مليون ليرة سورية.

3) إذا وقع الاحتيال على مصرف أو مؤسسة مالية.

ج-ولا تطبّق الأسباب المخفّفة التقديرية إلاّ إذا أسقط المضرور حقه الشخصي.)

لم يعرف المشرع السوري الاحتيال عبر الشبكة في قانون مكافحة الجريمة المعلوماتية، **ويمكن تعريفه بأنه: (الاستيلاء على مال الغير بالخداع عبر الشبكة أو الأجهزة الحاسوبية).**

فالاحتيال يتمثل في قيام الجاني بخداع المجني عليه بوسيلة معلوماتية، فيقع هذا الأخير في الغلط ويسلّم ماله إلى الجاني.

وسنتناول الركن المادي والركن المعنوي للاحتيال عبر الشبكة ثم سنسلط الضوء على عقوبته البسيطة والمشددة.

أ–الركن المادي:

يتكون الركن المادي في جريمة الاحتيال عبر الشبكة من ثلاثة عناصر: النشاط الجرمي، والنتيجة الجرمية، وعلاقة السببية.

فالنشاط الجرمي للاحتيال عبر الشبكة يتمثل في **فعل الخداع** الذي يمارسه الجاني حيال المجني عليه أو حيال منظومته المعلوماتية عبر الشبكة أو الأجهزة الحاسوبية. أما **النتيجة** فتتمثل بتسليم المجني عليه ماله أو ما في حكمه إلى المحتال تحت وطأة الخداع. و**علاقة السببية** التي تقتضي أن يكون تسليم المال بسبب الخداع.

والواقع أن الاحتيال التقليدي لا يختلف عن الاحتيال عبر الشبكة إلا في أن هذا الأخير يشمل **بموضوعه** المعلومات والبرامج والامتيازات المالية، وأن **النشاط الجرمي** المتمثل **بفعل الخداع** يمكن أن يقع على المجني عليه أو على منظومته المعلوماتية، وأن الخداع **ليس له وسائل محددة** كالاحتيال التقليدي، بالإضافة إلى أنه يرتكب عبر الشبكة أو الأجهزة الحاسوبية.

و يقصد بموضوع الاحتيال "ذلك الشيء الذي يرد عليه التسليم الصادر من المجني عليه إلى المحتال نتيجة الغلط الذي أوقعه فيه"[(32)].

وقد حدّد المشرع السوري **موضوع الاحتيال** بالمادة 21 من قانون الجريمة المعلوماتية بأنه: (مال منقول أو عقار، أو معلومات أو برامج ذات قيمة مالية، أو سند يتضمّن تعهداً أو إبراء أو أي امتياز مالي آخر).

ويقصد بالمال، كل شيء يصلح محلاً لحق عيني، وعلى وجه التحديد حق الملكية[(33)]. ويُشترط في المال أن يكون ذا طبيعة مادية، أي قابلاً للحيازة والتسليم و التملك. و الشيء المادي هو "كل ماله كيان ذاتي مستقل في العالم الخارجي، أو هو كل ماله طول وعرض

(32) د.محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، الطبعة الثالثة، منشورات الحلبي الحقوقية،بيروت، عام 1998، المجلد الأول، ص 382.

(33) د.محمود نجيب حسني، المرجع السابق، ص34 و 384. د.علي القهوجي: قانون العقوبات – القسم الخاص، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت عام 2001، ص802.

وسمك، بصرف النظر عن حجمه أو وزنه أو هيئته"[34].

ومتى اكتسب الشيء صفة المال؛ فإنه يصلح موضوعاً للاحتيال عبر الشبكة، كالنقود، أو المنقولات، أو العقارات، أو الإسناد التي تتضمّن تعهداً أو إبراءً، أو المعلومات أياً كان نوعها أو البرامج ذات القيمة المالية، أو أي امتياز مالي آخر. وهنا يظهر الفرق بين الاحتيال التقليدي والاحتيال عبر الشبكة، فالاحتيال التقليدي لا يشمل سوى المال المادي، أما الاحتيال عبر الشبكة فيشمل بالإضافة إلى المال المادي، **المعلومات، و البرامج ذات القيمة المالية، و الامتيازات المالية**. وبهذا يكون المشرع السوري قد أضفى على المعلومات أو البرامج **صفة المال المادي**، فالمعلومات والبرامج **لها قيمة** تصل إلى حد الثروات الطائلة، وهي نتاج الإبداع الفكري، و تُباع وتُشترى وتُقوّم بالمال، وكل شيء له قيمة يكتسب صفة المال، ويصلح لأن يكون محلاً للملكية. أضف إلى ذلك أن **المادة** هي كل ما يشغل حيزاً مادياً في فراغ معين، بحيث يمكن قياس هذا الحيز والتحكم فيه، فالبرامج أو المعلومات تشغل حيزاً مادياً في ذاكرة الحاسوب، ويمكن قياسه بمقياس معين هو البايت (BYTE)، فحجم أو سعة ذاكرة الحاسوب تقاس بعدد الحروف التي يمكن تخزينها فيها، إضافة إلى أن البيانات تكون على شكل إشارات إلكترونية ممثلة بالرقمين (0 أو 1)، وهي في ذلك تشبه التيار الكهربائي الذي اعتبرته بعض التشريعات من الأشياء المنقولة[35]. أما **الامتياز المالي** فيقصد به أي نوع من أنواع **المنفعة** التي يمكن أن يحصل عليها المحتال، كما لو استطاع أن يحصل على تذكرة حضور مسرحية عن طريق الاحتيال عبر الإنترنت. وغني عن البيان أنه يشترط في موضوع الاحتيال أن يكون مملوكاً للغير، لأنه لا يتصور الاعتداء على حق الملكية إلاّ إذا كان المال موضوع الاعتداء غير مملوك للمحتال، فإذا كان مملوكاً له أو غير مملوك لأحد، كالمال المباح، فلا يمكن تصور الاعتداء على الملكية الذي تتطلبه جريمة الاحتيال.

أما النشاط الجرمي للاحتيال فيتمثل بالخداع، و **يقصد بفعل الخداع** "تغيير الحقيقة في واقعة ما، تغييراً من شأنه إيقاع المجني عليه في غلط يدفعه إلى تسليم ماله إلى الجاني"[36].

---

(34) د.علي القهوجي: المرجع السابق، ص664.

(35) علي حسن محمد الطوالبة: التفتيش الجنائي على نظم الحاسوب والإنترنت (دراسة مقارنة)، رسالة دكتوراه مقدمة إلى جامعة عمان العربية، كلية الدراسات القانونية العليا، 2003، ص30. د.علي محمود علي حمودة: الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، المنعقد في دبي من 26–28 نيسان 2003، ص 23. متوفر على الموقع www.arablawifo.com، و راجع أيضاً الفقرة الثانية من المادة 621 من قانون العقوبات التي تنزل القوى المحرزة منزلة الأموال المنقولة.

(36) د.علي القهوجي: المرجع السابق، ص762.

فجوهر الخداع هو الكذب الذي يتخذه الجاني حيال المجني عليه، ولم يشترط المشرع السوري في جريمة الاحتيال عبر الشبكة أن يقترن الكذب بوسيلة احتيالية محددة كما فعل في الاحتيال التقليدي بالمادة 641 من قانون العقوبات، **وإنما اكتفى بأن يتم الخداع بأي وسيلة كانت**، فأي وسيلة تعطي الكذب الذي يدعيه المحتال مظهر الحقيقة تكفي لتكوين الخداع، كاتخاذ المحتال عبر الإنترنت مظهر الرجل الثري من خلال وضع صور وهمية لمنزله أو سيارته الفاخرة أو وضعه لعناوين وهمية لشركاته التجارية التي يدعي ملكيتها، أو انتحاله شخصية فتاة جميلة أو صفة طبيب مرموق وغير ذلك. فشبكة الإنترنت تقدم للمحتالين القدرة على الاتصال الإلكتروني بملايين الضحايا حول العالم بكلفة أقل بكثير من وسائل الاتصال التقليدية كالهاتف. كما تقدم له القدرة على إخفاء هوياتهم الحقيقة، الأمر الذي يجعل من الصعب ملاحقتهم ومحاكمتهم[37].

وفي مجال الاحتيال عبر الشبكة يثور التساؤل التالي: **هل يمكن أن يقع الخداع على الحاسوب بوصفه آلة؟** فمثلاً إذا قام الجاني عن طريق الإنترنت بالدخول إلى منظومة معلوماتية عائدة لأحد المصارف، وقام بخداع هذا النظام عن طريق التلاعب ببياناته بغية تحويل أموال عائدة للغير إلى حسابه، **فهل يتحقق هنا فعل الخداع؟**

إن الإجابة على هذا السؤال كانت محل خلاف في الفقه والتشريع المقارن[38]، وقد حسم المشرع السوري هذا الخلاف عندما نص صراحة في المادة 21 من قانون الجريمة المعلوماتية على أن **الخداع يمكن أن يقع على المجني عليه أو على منظومة معلوماتية خاضعة لسيطرته**. وبالتالي فإن فعل الخداع يمكن أن يقع على النظم المعلوماتية،لأن الحاسوب ليس سوى وسيط يعبّر عن إرادة المجني عليه، فهذا الأخير هو من يقوم ببرمجته وفقاً لمتطلباته، وبالتالي فخداع الحاسوب هو خداع للمجني عليه.

أما **النتيجة الجرمية** لجريمة الاحتيال عبر الشبكة فقد حددها المشرع بأنها **(الاستيلاء على مال المجني عليه)** وفق مفهوم المال الذي سبق بيانه. وعلى ذلك فإن النتيجة الجرمية هي **التسليم** الصادر عن المجني عليه للمحتال تحت تأثير الغلط الذي أوقعه به، ثم قيام المحتال **بالاستيلاء** على هذا المال. كما يجب أن تتوافر **الصلة السببية** بين الخداع والتسليم، بحيث يمكن القول أنه لولا الخداع لما تمّ التسليم.

وفي مجال الاحتيال عن طريق التحويلات المصرفية، فقد استخدمت الإنترنت للولوج إلى أنظمة المصارف، والقيام بتحويلات مالية من حسابات العملاء إلى حسابات الهكرة. فقد استطاع

(37) Richard Hillman: securities fraud, The internet poses challenges to Regulateres and Investors, United States General Accounting Office, 1999, P4.

(38) د. محمد طارق الخن، المرجع السابق، ص153 وما بعدها.

الهكرة الروس ارتكاب خمسمائة عملية استيلاء على مصرف روسيا المركزي خلال الفترة مابين عام 1994 إلى 1996، وقاموا بتحويل مبالغ تصل إلى مائتين وخمسين مليون روبل إلى حساباتهم الخاصة. وكان المدعو "فلاديمير ليفين" وهو مبرمج حاسوب عمره 29 عاماً، أحد أقوى الهكرة الروس الذي اخترق شبكة حاسوب مصرف "ستي بنك" "Citibank" بولاية نيوجرسي الأميركية، واستولى على عدة ملايين باستخدام حاسوبه المحمول أثناء وجوده في روسيا، وبلغت قدرة هذا الهاكر أنه استطاع مراقبة التحويلات والصفقات المالية التي تتم بالمصارف، ثم قام بتحويلات مالية من حسابات عملائها إلى حسابات خاصة به سبق وأن فتحها في مصارف هولندا وفنلندا وألمانيا والولايات المتحدة، حيث وصلت قيمة التحويلات المالية المختلسة من قبله إلى اثني عشر مليون دولار أميركي. وقد أُلقي القبض عليه في إنكلترا وتمّ تسليمه إلى الولايات المتحدة الأميركية، حيث صدر بحقه حكم بالسجن مدة ثلاث سنوات في عام 1998[39].

وفي مثال آخر، أنه في 27 كانون الأول عام 2000 حكم قاضٍ فيدرالي في مقاطعة كاليفورنيا بالسجن لمدة سبعة وعشرين شهراً وبمبلغ مئة ألف دولار تعويضاً للضحايا، على مجموعة من الأفراد قاموا بالاحتيال التجاري عبر الإنترنت، حيث أرسلوا أكثر من /50/ مليون رسالة إلكترونية دعائية إلى الطلاب وكبار السن، طلبوا فيها الحصول على المال مقابل العمل في المنازل، وتضمنت هذه الرسائل الوعود بالعمل بالمنازل مقابل دفعات مالية، وقد أرسل معظم الضحايا المال إلى المتهمين. كما وضع المتهمون في رسائلهم عنوان بريد مزوّر لتضليل المجني عليهم، يُظهر بأن الرسائل أرسلت من مزود خدمة الإنترنت Big Bear.net، وبعد ذلك أرسل المجني عليهم الغاضبون إلى موقع مزود الخدمة المذكور أكثر من /100.000/ رسالة إلكترونية، لاعتقادهم الخاطئ بأنه هو المسؤول عن الاحتيال، الأمر الذي أدّى إلى تعطل مزود الخدمة نتيجة هذا العدد الكبير من الرسائل. وقد استعانت شركة Big Bear بثلاثة موظفين مؤقتين للرد على هذه الرسائل لمدة /6/ أشهر. كما شمل قرار المحكمة التعويض على الشركة المذكورة إضافةً إلى الضحايا [40].

ومن أمثلة الاحتيال التجاري عبر الإنترنت أنه في 10 أيار عام 2001، أدانت هيئة المحلفين الاتحادية في مقاطعة "كولورادو" المتهم "دانيال كتلسن"Daniel Ketelsen بالاحتيال عبر الإنترنت، حيث قام "كتلسن" باستعمال اسماً كاذباً واستلام المال كثمن لقطع حاسوب عرضها للبيع من خلال موقع e-bay، ولكنه لم يقم بتسليم البضائع. وبعد استلام الكثير من

(39) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص409.

(40) On line fraud and crime ,Are consumers safe? Hearing before the subcommittee on commerce trade and consumer protection, 2001, P 33.

الشكاوى بحق "كتلسن"، قام هذا الأخير برفع شكوى ضد شركة التأمين، زاعماً أن البضاعة سرقت من مرآبه، ولكن التحقيق الذي قام به المحققون في مؤسسة البريد الأمريكية، كشف أن "كتلسن" لا يملك أية بضاعة، وأنه كان يحاول أيضاً الحصول على المال بشكل غير شرعي من شركة التأمين[41].

وفي قضية أخرى، تم استدعاء أربعة متهمين إلى المحكمة بتهمة الاحتيال عبر الإنترنت في جورجيا، وذلك لقيامهم بالاحتيال عبر موقع e-bay، حيث قاموا باستخدام الموقع لبيع إطارات السيارات، وقام الزبائن بالتفاوض على السعر والدفع عن طريق تحويل الأموال عبر الإنترنت، أو عبر موقع "ويسترن يونين" western union، ولكن البضائع لم ترسل للضحايا. ومنذ تموز عام 2003 حتى تشرين الأول عام 2006، دفع حوالي 215 شخص للمتهمين ما يعادل 539.000 دولار ثمناً لبضائع لم يتم إرسالها[42].

ولتفادي عمليات الاحتيال عند الشراء عبر الإنترنت، فإن هذه الشبكة تقدم خدمة يطلق عليها Escrow House، وهي عبارة عن مؤسسات مالية تُرسل إليها النقود التي يراد شراء المنتجات بها من أي موقع إلكتروني، حيث تقوم بتجميد الأموال لديها حتى يصلها إخطار من المشتري بأنه قد تسلم المنتجات التي طلبها، وأنها مطابقة للمواصفات المطلوبة. عند ذلك تقوم هذه المؤسسات بتحويل الأموال إلى المواقع التي تم الشراء منها. وفي حال عدم وصول المنتجات التي طلبها العميل، أو كانت غير مطابقة للمواصفات، فإنه يمكن استرداد هذه الأموال[43].

ومن أشكال الاحتيال عبر البريد الإلكتروني، **أسلوب العروس الروسية**. ويعرف بهذا الاسم، لأن مرتكبي هذا الأسلوب هم رجال من روسيا في أغلب الأحيان. ومن أشهر المحتالين في هذا المجال، رجل روسي في الأربعين من عمره، اسمه "روبرت ماك كوي" Robert Mc Coy، الذي كان يتعرف على ضحاياه، عن طريق الإعلانات الشخصية التي ينشرها عن نفسه عن طريق بعض المواقع الإلكترونية، مثل America on line. وقد كان "روبرت" ينتحل في رسائله الإلكترونية صفة امرأة روسية تبحث عن الحب، ويقوم بإرسال صور لعارضة جميلة إلى ضحيته. وتستمر هذه العلاقة لفترة من الزمن، ثم يقوم بإخبار الضحية بأن الفتاة الجميلة ترغب برؤية عشيقها، وتحتاج إلى مبلغ /1800/ دولار أميركي لتغطية مصاريف التأشيرة وتذكرة

(41) On line fraud and crime ,op-cit, p.33.

(42) IC3, op-cit, p-15

(43) ومن مواقع هذه المؤسسات www.iescrou.com د.جميل عبد الباقي الصغير: الإنترنت والقانون الجنائي، دار النهضة العربية، القاهرة،2002، ص39.

الطائرة. وبعد أن يتم إرسال هذا المبلغ، وفي اليوم الذي يتوقع فيه الضحية وصول الفتاة الجميلة، تصله رسالة منها تدعي فيها، أن هناك مشكلة تتعلق بالقوانين الروسية الحديثة التي لا تسمح لها بالمغادرة إلاّ إذا كان معها /1500/ دولار أميركي نقداً، وبعد أن يرسل الضحية هذا المبلغ. يتم تجاهل رسائله الإلكترونية، أو تُعاد إليه رسائله لأن حسابات المشتركة الروسية قد أُغلقت. عندها يعلم أنه وقع ضحية عملية احتيال.

وبعد إلقاء القبض على "ماك كوي"، اعترف بالاحتيال على أكثر من /250/ رجلاً، كان معظمهم من الولايات المتحدة الأميركية، وحصل منهم على ما يزيد على مليون دولار أميركي، وقد حُكم عليه بالسجن مدة خمس سنوات(44).

ب–الركن المعنوي:

جريمة الاحتيال عبر الشبكة لا تختلف عن جريمة الاحتيال التقليدي لجهة الركن المعنوي فهي جريمة مقصودة، ومن ثم فالركن المعنوي يتخذ فيها صورة القصد الجرمي. والقصد الجرمي المطلوب للاحتيال هو القصد العام فقط(45).

ويذهب بعض الفقهاء إلى أن القصد الجرمي المطلوب توافره في جريمة الاحتيال، هو القصد الجرمي العام والقصد الجرمي الخاص، ووفقاً لهذا الرأي فإن مضمون القصد الخاص هو "نية التملك"(46).

وفي تقديرنا أن القصد الخاص لا يلزم توافره إلى جانب القصد العام لتحقق الركن المعنوي في جريمة الاحتيال، لأن نيّة التملك تدخل في عناصر القصد العام، الذي تتجه الإرادة فيه إلى النشاط الجرمي والنتيجة. فالنتيجة الجرمية في جريمة الاحتيال تتمثّل في تسليم المال، ويُقصد بهذا التسليم تمكين المحتال من السيطرة على المال محل التسليم سيطرةً تسمح له بالاستيلاء عليه، أي أن يحوزه حيازة كاملة بعنصريها المادي والمعنوي، وهذه الحيازة هي التي تسمح للجاني أن يمارس على هذا المال مظاهر السيطرة التي ينطوي عليها حق الملكية. وبالتالي فلا حاجة لجعل نيّة التملك مستقلة ضمن القصد الخاص.

---

(44) هذه القضية متوفرة على الموقع www.russian-detective . com/scams وقضية أخرى:
Joseph T. wells, Computer Fraud Casebook, Published by John Wiely @sons. Inc, Hoboken, New Jersey, 2009, P 35 - 45.

(45) من هذا الرأي د.علي القهوجي: المرجع السابق، ص814. د. علاء عبد الباسط خلاف: الحماية الجنائية لوسائل الاتصال الحديثة، دار النهضة العربية، القاهرة، 2002، ص107.

(46) ومن هذا الرأي د. محمود نجيب حسني: جرائم الاعتداء على الأموال في قانون العقوبات اللبناني، المرجع السابق، ص392. د.أحمد حسام طه تمام: المرجع السابق، ص549. د. نائلة قورة: المرجع السابق، ص489.

والقصد العام يتكون من عنصرين هما: العلم والإرادة، أي العلم بجميع عناصر الركن المادي، وإرادة تتجه إلى السلوك والنتيجة الجرمية.

فيجب أن يعلم الجاني بأنه يرتكب فعل الخداع، وأن هذا الفعل يؤدي إلى إيقاع المجني عليه في الغلط حيث يحمله على تسليم ماله. كما يجب أن تتجه إرادة الجاني إلى النشاط الجرمي وهو الخداع. وأن تتجه إرادته أيضاً إلى تحقيق النتيجة الجرمية وهي استلام المال من المجني عليه، ثم الاستيلاء عليه والظهور بمظهر المالك "نية التملك".

ج- عقوبة الاحتيال البسيط والمشدد:

حدد المشرع **عقوبة الاحتيال البسيط عبر الشبكة** بالفقرة (أ) من المادة 21 من قانون مكافحة الجريمة المعلوماتية بالحبس من ثلاث إلى خمس سنوات والغرامة من خمسمئة ألف إلى مليونين ونصف مليون ليرة سورية.

ثم شدد العقوبة في الفقرة (ب) إلى الاعتقال المؤقّت، والغرامة من خمسمئة ألف إلى مليونين ونصف مليون ليرة سورية، في الحالات التالية:

1- إذا وقعت الجريمة على ثلاثة أشخاص فأكثر.

2- إذا تجاوز مبلغ الضرر مليون ليرة سورية.

3- إذا وقع الاحتيال على مصرف أو مؤسسة مالية.

و علة التشديد في هذه الظروف الثلاثة واضحة وهي خطورة الجاني عندما يتعدد المجني عليهم، أو عندما يكون حجم الضرر كبيراً، أو عندما يكون المجني عليه ذو صفة مصرفية.

كما منع المشرع في الفقرة (ج) من هذه المادة المحكمة من الأخذ بالأسباب المخفّفة التقديرية إلاّ إذا أسقط المضرور حقه الشخصي.

ثامناً: الاستعمال غير المشروع لبطاقات الدفع:

شاع في الآونة الأخيرة استعمال بطاقات الدفع على اختلاف أنواعها، وذلك من أجل التيسير على الأفراد في معاملاتهم المالية. وقد ساعدت الثورة المتسارعة لنظم الحوسبة ونظم الاتصالات وخاصة الشبكات على نقل المعلومات عبر العالم خلال لحظات معدودات، فأصبحت هذه البطاقات أكثر وسائل الدفع استخداماً وانتشاراً محلياً وعالمياً، وقد ربطت الشبكات

وخاصة الإنترنت المصارف بنقاط البيع الإلكترونية وأجهزة سحب النقود أينما وجدت.

وقد صاحب انتشار هذه البطاقات وتزايد حجم التعامل بها، نمواً مضطرداً في الجرائم المرافقة لاستخدامها، كالاستيلاء على بياناتها و أرقامها، وتزويرها، و استعمال البطاقات المزورة أو المسروقة أو المفقودة وغير ذلك من أشكال الإجرام.

وقد جرم المشرع السوري الاستعمال غير المشروع لبطاقة الدفع في المادة 22 من قانون مكافحة الجريمة المعلوماتية التي نصت على ما يلي:

(أ-يُعاقَب بالحبس من ثلاثة أشهر إلى سنتين والغرامة من خمسمئة ألف إلى مليونين ونصف مليون ليرة سورية، كل من حصل دون وجه حق على بيانات أو أرقام بطاقة دفع باستخدام الأجهزة الحاسوبية أو الشبكة.

ب -يُعاقَب بالحبس من ثلاث إلى خمس سنوات والغرامة من خمسمئة ألف إلى مليونين ونصف مليون ليرة سورية، كل من:

1- قام بتزوير بطاقة دفع.

2- استعمل بطاقة دفع مزوّرة أو مسروقة أو مفقودة في الدفع أو سحب النقود.)

وقبل الدخول في صور هذا الإجرام لابد لنا من التعرف أولاً على ماهية بطاقة الدفع وأنواعها، ثم سنتناول جريمة الحصول دون وجه حق على بيانات أو أرقام بطاقة الدفع، ثم سننتقل لدراسة تزوير هذه البطاقات، ومن ثم استعمال البطاقة المزورة أو المسروقة أو المفقودة.

أ- ماهية بطاقة الدفع:

عرف المشرع السوري في المادة الأولى من قانون مكافحة الجريمة المعلوماتية **بطاقة الدفع** بأنها: (بطاقة ذات أبعاد قياسية، تصدرها عادة المصارف أو المؤسسات المالية وما بحكمها، وتُستخدم في عمليات الدفع أو الائتمان أو سحب الأموال أو تحويلها عن طريق حساب أو محفظة مصرفية)

وبطاقة الدفع هي عبارة عن بطاقة مستطيلة الشكل ذات أبعاد قياسية، مصنوعة غالباً من مادة البلاستيك، ومسجل على وجهيها مجموعة من البيانات الأساسية وهي[47]:

1- اسم وشعار المنظمة الدولية (فيزا Visa، ماستر كارد Master Card....)

---

(47) د. جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، المرجع السابق،ص12. وائل الدبيسي: البطاقة المصرفية، مطبعة صادر- بيروت، عام 2004، ص33.

Robin Bryant, op- cit, p- 136 .

2– اسم وشعار المصرف المصدر: وهو المصرف الذي يحق له إصدار البطاقات، مثل المصرف التجاري السوري الذي يقوم بإصدار بطاقات الفيزا في سورية.

3– رقم البطاقة: وهو الرقم المطبوع على صدر البطاقة، وهو رقم تعريف مكون من 16 خانة، ولا يُعطى عشوائياً، وإنما وفقاً لمعادلة رياضية معينة، ويسمى هذا الرقم (pan)[48].

4– اسم حامل البطاقة.

5– تاريخ الإصدار.

6– تاريخ الصلاحية.

7– صورة حامل البطاقة في بعض أنواع البطاقات.

8– الشريط الممغنط: وهو شريط ممغنط يقع على ظهر البطاقة وعلى طولها، مسجل عليه بيانات غير مرئية يمكن قراءتها بواسطة أجهزة الصراف الآلي ATM،أو عن طريق نقاط البيع التي تتضمن آلة إلكترونية تعرف بـ POS مخصصة لذلك[49]. وهذه البيانات هي التي يحتاجها الحاسوب للتعرف على رقم البطاقة والحد المسموح به للسحب، والرقم الشخصي، والتواريخ والرموز الأخرى الخاصة بالمعاملات التجارية.

9– شريط التوقيع: وهو شريط يقع على ظهر البطاقة، حيث يقوم حامل البطاقة بالتوقيع عليه أمام موظف المصرف مصدر البطاقة عند تسلمه لها. والفائدة من وجود توقيع الحامل على هذا الشريط هي تمكين التاجر المتعامل مع حامل البطاقة من التأكد من هوية هذا الأخير عن طريق مضاهاة التوقيع الموجود على البطاقة مع توقيع الحامل أمامه.

10– رقم التعريف الشخصي: وهو رقم سري لا يظهر على البطاقة، ويتكون عادة من أربع خانات، ويرمز له بـ pin[50]، ويسلم هذا الرقم للعميل في ظروف مغلق عند استلامه للبطاقة، وذلك ليستخدمه عند السحب من الصراف الآلي، أو عند الشراء من نقاط البيع الإلكترونية. ويعد هذا الرقم صورة مبسطة من صور التوقيع الإلكتروني.

ويمكن التمييز هنا بين نوعين من البطاقات البلاستيكية حسب طريقة تصنيعها، هما:

---

(48) وهو اختصار لـ Primary account Number

(49) ATM هو اختصار لـ Automatic Teller Machine والمقصود بها جهاز الصراف الآلي، أما POS فهو اختصار لـ Point Of Sale أي نقطة البيع.

(50) وهو اختصار لـ Personal Identification Number

النوع الأول: البطاقة الممغنطة التقليدية Swipe Card:

وهي البطاقة المغناطيسية التي تكون فيها المعلومات مخزنة على الشريط الممغنط الذي أشرنا إليه سابقاً.

النوع الثاني: البطاقات الذكية Smart Card:

وهذه البطاقات تشبه الحواسيب المصغرة، لأنها تقوم بعدة عمليات حسابية، وهي عالية الأمان ولا يمكن تزويرها.

ويمكن التمييز بين نوعين من هذه البطاقات، فهناك بطاقات ذكية تحوي على بطاقة ذاكرة، وبطاقات ذكية أخرى تحوي على رقاقة معالجة.

أما البطاقات الذكية ذات الذاكرة، فهي تحتفظ بالمعلومات على ذاكرة قابلة لإعادة الكتابة. ومن أمثلة هذه البطاقات، بطاقات الهواتف العادية التي تستعمل في الهواتف العمومية، وفيها تقوم الذاكرة بتسجيل الزمن والمبلغ المتبقي في كل مرة يتم استعمالها.

أما البطاقات الذكية ذات الرقاقة، فهي أكثر تعقيداً، وهي تحتوي على معالج يتضمن ذواكر حية وساكنة Rom and Ram، ومن أمثلة هذه البطاقات، بطاقات الائتمان والديون [51].

ب- أنواع بطاقات الدفع [52]:

يمكن تقسيم بطاقات الدفع حسب وظائفها إلى الأنواع التالية:

1- بطاقات سحب النقود:

جميع بطاقات الدفع تتمتع بوظيفة سحب النقود، إلا أن بعض أنواعها تقتصر على هذه الوظيفة، وقد تخول هذه البطاقة حاملها وظيفة سحب النقود داخل القطر الواحد، أو سحب النقود في الخارج، وذلك ضمن الحد الأقصى المحدد المسموح بسحبه يومياً أو أسبوعياً. ويسجل المبلغ المسحوب في الجانب المدين من حساب العميل مباشرة (on- line).

2- بطاقات الوفاء Debit Card:

وهي البطاقة التي تسمح لحاملها بوفاء ثمن السلع والخدمات التي يحصل عليها من التجار المتعاملين بها دون حاجة للوفاء نقداً. فبواسطة هذه البطاقة يستطيع التاجر أن يستوفي

(51) Robin Bryant, op- cit, p- 134.

(52) د. نائلة قورة: المرجع السابق، ص508. وائل الدبيسي: المرجع السابق، ص34. د. جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، المرجع السابق، ص15. د.الفتاح بيومي حجازي: التجارة الإلكترونية وحمايتها القانونية، دار الفكر الجامعي، الإسكندرية، عام 2004، الكتاب الأول، ص111.

ثمن السلع أو الخدمات عن طريق المصرف المصدر للبطاقة بطريقتين: إحداهما غير مباشرة والأخرى مباشرة.

ففي الطريقة غير المباشرة، يقدم فيها العميل بطاقته إلى التاجر، الذي يقوم بالحصول على بيانات البطاقة من خلال تمريرها على آلة يدوية، تحتوي على ثلاثة إشعارات بيع، ثم يقوم العميل بالتوقيع على هذه الإشعارات أو الفواتير، حيث يتم إرسال إحدى هذه النسخ إلى مصرف العميل لتسديد قيمة المشتريات.

أما الطريقة المباشرة، فيقدم فيها العميل بطاقته إلى التاجر، حيث يمرر هذا الأخير البطاقة على آلة إلكترونية ترتبط بالمصرف الذي يتعامل معه، وذلك من أجل التأكد من وجود رصيد كافٍ للعميل في المصرف حتى يستطيع التاجر الحصول على قيمة المشتريات. و هنا لا تتم هذه العملية إلا بعد قيام العميل بإدخال رقمه السري في هذه الآلة، فإذا كان رصيد العميل كافياً تتم عملية التحويل مباشرة من حساب العميل إلى حساب التاجر عن طريق عمليات حسابية في مصرف كل منهما، وإلا ترفض العملية.

وتنقسم بطاقات الوفاء حسب علاقة حامل البطاقة بمصدرها إلى نوعين، هما:

بطاقات الاستيفاء الفوري، وهي بطاقة لا يستفيد الحامل فيها من مهلة للوفاء، ويكون دور البطاقة هنا أداة وفاء فقط، إذ تتطلب هذه البطاقة أن يقوم حاملها بتزويد حسابه برصيد كافٍ دائماً، لأن استيفاء ما يحصل عليه الحامل من سلع أو خدمات يتم فوراً من حسابه دون انتظار، أي دون منح مهلة للوفاء.

أما النوع الثاني فهو **بطاقات الاستيفاء المؤجل**، وهي بطاقات تُستخدم كأداة وفاء وأداة ائتمان، حيث تسمح للحامل بوفاء ثمن ما حصل عليه من سلع وخدمات مستفيداً من مهلة زمنية، وهي الفترة الواقعة بين تاريخ تنفيذ المشتريات وتاريخ الوفاء. وهذه المهلة لا تتعدى عادة ستة أسابيع.

3- بطاقات السداد المؤجل أو بطاقات الائتمان Credit Card(53) أو بطاقات الاعتماد:

وهي تسمح لحاملها باستعمال ائتمان في حدود الاتفاق المبرم بينه وبين المصرف المصدر. فبدلاً من أن يقوم حاملها بتسوية حسابه فوراً، فإنه يستطيع أن يسدد ثمن مشترياته

(53) يطلق معظم الفقهاء مصطلح بطاقات الائتمان بصفة عامة على جميع أشكال البطاقات على اختلاف أنواعها، على الرغم من أن بطاقة الائتمان هي واحدة من هذه الأنواع.

على دفعات خلال أجل متفق عليه مع المصرف، وذلك في حدود مبلغ مكشوف معين مسبقاً. فحامل هذه البطاقة يُفترض أن يكون مديناً، إلا أنه في حاجة إلى الحصول على السلع والخدمات التي يقوم المصرف بتسديد ثمنها إلى التاجر، ثم يسترد ما دفعه من حامل البطاقة بعد ذلك.

والجهات المصدرة لهذه البطاقات تحصل على فوائد مقابل توفير اعتماد لحاملها. ولذلك فهذه البطاقات أداة ائتمان حقيقية، ويتحدد هذا الائتمان بحد أقصى لكل حامل تبعاً لائتمانه الشخصي. والمصارف لا تمنح هذه البطاقات إلا بعد التأكد من ملاءة العميل أو الحصول منه على ضمانات عينية أو شخصية كافية.

4- بطاقات ضمان الشيكات Cheque Guarantee Card:

يقتصر عمل هذه البطاقة على ضمان وفاء الشيكات، حيث يقوم التاجر بتدوين بياناتها الرئيسية على ظهر الشيك، بعد التأكد من تاريخ الصلاحية، وأن الشيك والبطاقة يحملان نفس اسم المصرف، ونفس رقم الحساب، ونفس التوقيع. و يقتصر الضمان الذي تقدمه هذه البطاقة للتاجر على حدود معينة يجب عليه عدم تجاوزها، وإلا سقط الضمان عن كامل المبلغ.

و بعد أن ذكرنا أنواع بطاقات الدفع والمزايا التي تقدمها، لابد لنا من الإشارة إلى أنه يمكن استخدام بطاقات الدفع للحصول على السلع والخدمات عن طريق الإنترنت؛ فحامل البطاقة يمكن أن يدخل إلى الموقع الإلكتروني للمتجر المرغوب فيه، ثم يقوم باختيار السلع المراد شراؤها، وعند ذلك يظهر على الشاشة نموذج يتضمن خانات فارغة متعلقة ببيانات بطاقة الدفع، حيث يقوم المشتري بملء هذه الخانات بالبيانات المتعلقة ببطاقته وعنوانه، ثم يتم استيفاء قيمة السلع من بطاقة الدفع، وإرسال هذه السلع إلى عنوان المشتري.

وغني عن البيان مدى الخطورة التي يمكن أن يتعرض لها حامل البطاقة عند إرساله لبيانات بطاقته عبر الإنترنت، وخاصة رقمها السري، وما يترتب على ذلك من إمكانية الاستيلاء على هذه البيانات، الأمر الذي قد يؤدي إلى خسارة مادية جسيمة لأصحاب البطاقات والمصارف معاً.

جريمة الحصول دون وجه حق على بيانات أو أرقام بطاقات الدفع

نصت الفقرة أ من المادة 22 من قانون مكافحة الجريمة المعلوماتية على ما يلي:

(أ- يُعاقَب بالحبس من ثلاثة أشهر إلى سنتين والغرامة من خمسمئة ألف إلى مليونين ونصف مليون ليرة سورية، كل من حصل دون وجه حق على بيانات أو أرقام بطاقة دفع باستخدام الأجهزة الحاسوبية أو الشبكة.)

وسنتناول الركن المادي والركن المعنوي لهذه الجريمة.

أ- الركن المادي:

يتمثل النشاط الجرمي في جريمة الاستيلاء أو الحصول دون وجه حق على بيانات أو أرقام بطاقة دفع، بقيام الجاني بأي فعل من شأنه أن يؤدي للحصول دون وجه حق على هذه البيانات أو الأرقام السرية لبطاقات الدفع. فلا تقوم هذه الجريمة إذا كان الحصول على هذه البيانات أو الأرقام بحق أو بصورة مشروعة أي بإرادة صاحب البطاقة. **ويشترط المشرع أن يتم الاستيلاء على بيانات أو أرقام بطاقة دفع باستخدام الأجهزة الحاسوبية أو الشبكة**، فلا تقوم هذه الجريمة إذا تم الحصول على هذه البيانات أو الأرقام عن طريق النشاط الذهني المحض وذلك لصعوبة الإثبات، كمشاهدة خادمة المنزل للورقة التي كتب عليها الرقم السري للبطاقة العائدة لرب عملها، أو مشاهدة الرقم السري للبطاقة من قبل الغير أثناء إدخاله عبر جهاز الصراف الآلي، ففي هذه الحالات لا تقوم هذه الجريمة لأن الحصول على الأرقام السرية لم يكن عن طريق بذل النشاط باستخدام الأجهزة الحاسوبية أو الشبكة. مع الأخذ بعين الاعتبار أنه من الممكن في حال استخدام هذه الأرقام أن يسأل الفاعل عن جريمة استعمال بطاقة الغير المنصوص عليها في الفقرة ب من المادة 22 المشار إليها.

أما **النتيجة الجرمية** فتتمثل في حصول الفاعل دون وجه حق على بيانات أو أرقام بطاقة دفع، ثم لا بد من قيام علاقة سببية بين سلوك الفاعل وهذه النتيجة.

وهناك العديد من أساليب الاستيلاء على البيانات والأرقام السرية لبطاقات الدفع باستخدام الأجهزة الحاسوبية أو الشبكة، ومن أبرز هذه الأساليب:

1- أسلوب انتحال الصفة:

و قد سبقت الإشارة إلى هذا الأسلوب الذي يتم عن طريق إنشاء مواقع مزيفة على شبكة الإنترنت، على غرار مواقع الشركات والمؤسسات التجارية الأصلية الموجودة على هذه الشبكة،

بحيث يبدو هذا الموقع المزيف وكأنه الموقع الأصلي المقدّم لتلك الخدمة. وبعد إنشاء الموقع المزيف، يستقبل عليه الجناة جميع المعاملات المالية والتجارية التي يقدمها عادة الموقع الأصلي لعملائه عبر شبكة الإنترنت، فيتم استقبال الرسائل الإلكترونية الخاصة بالموقع الأصلي والاطلاع عليها، ومن ثم يتم الاستيلاء على البيانات الخاصة ببطاقات الائتمان أو بطاقات الدفع الإلكتروني(54).

2– **أسلوب التجسس:**

يقوم الجناة وفقاً لهذا الأسلوب باستخدام برامج لاختراق الأنظمة المعلوماتية للشركات والمؤسسات التجارية العاملة على شبكة الإنترنت، ومن ثم يستطيع هؤلاء الجناة الاطلاع على البيانات والمعلومات التجارية الخاصة بهذه الشركات، ومنها المعلومات المتعلقة ببطاقات الدفع الإلكترونية المستخدمة في التجارة الإلكترونية عبر الشبكة. و بذلك يتمكن الجاني من الاستيلاء على بيانات البطاقات الصحيحة، واستخدامها عبر شبكة الإنترنت على حساب الحامل الشرعي للبطاقة(55).

ومن أمثلة هذا الاختراق، ما حدث في عام 1996، حيث تم اختراق حاسوب محمول يحتوي على 314.000 رقماً لبطاقة ائتمان خاصة بأحد المكاتب التابعة لمؤسسة Visa Card INT في كاليفورنيا.

وفي عام1997، قام شخص يدعى "كارلوس سادالغو" Carlos Sadalgo، بالاستيلاء على أرقام 100.000 بطاقة ائتمان وبيانات أخرى، من خلال اختراقه لمجموعة من مزودي خدمات الإنترنت، وقام بوضع هذه الأرقام على أسطوانة مضغوطة، ثم قام بتشفيرها وعرضها للبيع بمبلغ مائتين وخمسين ألف دولار. ولقد اكتشف عملاء المباحث الفيدرالية هذه الجريمة، وحوكم "سادالغو" وعوقب بالسجن ثلاثين شهراً(56).

3– **أسلوب الشفط** Skimming(57):

"Skimming" هو طباعة التفاصيل المخزنة على الشريط الممغنط لبطاقة الدفع، عن طريق تمرير البطاقة على قارئ إلكتروني، وبمجرد الحصول على تفاصيل البطاقة، مثل رقم التعريف بهوية الحامل (PAN)، وتاريخ انتهاء صلاحية البطاقة، يستطيع المحتال إنشاء بطاقة

(54) د. جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة، المرجع السابق، ص37.

(55) د. جميل عبد الباقي الصغير: الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة،المرجع السابق، ص38.

(56) د. عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق، ص421.

(57) Robin Bryant, op- cit, p. 141-142.

مطابقة للبطاقة الأصلية، لاستعمالها في الصفقات التي تعقد على الإنترنت.

وأجهزة الـ "Skimmer" توضع مثلاً على فتحة الصراف الآلي، حيث يتم مسح تفاصيل بطاقة الزبون ضوئياً، وتخزينها في جهاز خاص قبل أو بعد دخول البطاقة إلى قارئ البطاقات في الصراف، وقد يرفق بالماسحة الضوئية كاميرا تسجل رقم PIN المُدخل من قبل الضحية.

وخطورة هذا النوع من الاستيلاء على بيانات البطاقات هو أن حامل البطاقة لا يعلم بأن بطاقته تم اختراقها، لذا لا يبلغ أحداً لإلغائها، وبذلك يستطيع المحتال استخدام البطاقة المزورة خلال فترة طويلة، وهذا بعكس الأسلوب التقليدي المتبع في الاستيلاء على بيانات البطاقة وهو سرقة البطاقة، لأنه في حال سرقة البطاقة يكون إمكانية استعمالها قصير الأمد، إذ إن الضحية ستلاحظ ذلك، وتقوم بتبليغ مصدر البطاقة لإلغائها.

ففي عام 2005، تمّ الحكم في إنكلترا على أربعة من أعضاء عصابة لمسح البطاقات وسحب الأموال، بالسجن لمدة أربع سنوات لارتكابهم الاحتيال الذي قدرت خسارته بـ 200,000 جنيه إسترليني.

كما تم التحذير من أسلوب Skimming، حيث وضعت تحذيرات على أجهزة السحب الآلي في معظم الدول، تتضمن الطلب من الزبائن عدم استخدامها إذا بدت غير طبيعية، وإذا كان هناك شك بوجود آلة Skimmer على جهاز سحب النقود، فإن الشرطة تنصح بعدم الإبلاغ فوراً لأن هذه الأجهزة غالية الثمن، وقد يتدخل المجرم تدخلاً عنيفاً في هذه الحالة. و لكن يمكن اعتقال هذا المجرم عندما يتم ترصده، لأنه سوف يعود لاسترجاع الجهاز.

ومن أكثر الحالات التي يمكن أن يستخدم بها جهاز Skimmer هي عند دفع الفواتير في المطاعم، حيث يقوم الزبون بإعطاء البطاقة إلى محاسب المطعم الذي يقوم بتمريرها على جهاز Skimmer ثم يقوم بإعادتها إلى صاحبها، وبذلك تتم عملية نسخ لبيانات البطاقة.

ومن الجدير بالذكر أن هناك أسلوباً ميكانيكياً للاستيلاء على بيانات بطاقات الائتمان، حيث يتم تحويل التفاصيل المنقوشة على البطاقة البلاستيكية ميكانيكياً من بطاقة إلى أخرى. وقد عرفت هذه التقنية بما يسمىShave And Paste. و هذه الطريقة أسهل من أسلوب سرقة البطاقة برمتها أثناء نقلها ما بين البنك والزبون.

4- <u>تخليق أرقام البطاقات Card Math:</u>

و يقوم هذا الأسلوب على تخليق أرقام بطاقات ائتمانية اعتماداً على إجراء معادلات رياضية وإحصائية، بهدف الحصول على أرقام بطاقات ائتمانية مملوكة للغير، وهي كل ما يلزم

للشراء عبر شبكة الإنترنت.

فهذا الأسلوب يعتمد على أسس رياضية في تبديل وتوفيق أرقام حسابية، تؤدي في النهاية إلى ناتج معين، وهو الرقم السري لبطاقة دفع متداولة، ثم يتم استخدامها استخداماً غير مشروع عبر شبكة الإنترنت[58].

ب- الركن المعنوي:

جريمة الحصول دون وجه حق على بيانات أو أرقام بطاقة دفع جريمة مقصودة تتطلب القصد الجرمي العام بعنصريه العلم والإرادة، أي علم الفاعل واتجاه إرادته إلى أي فعل من الأفعال التي تؤدي إلى الاستيلاء أو الحصول دون وجه حق على بيانات أو أرقام بطاقة دفع عائدة للغير ، وذلك باستخدام الأجهزة الحاسوبية أو الشبكة. فلا تقوم هذه الجريمة بحق من يطلع خطأً عبر الإنترنت على الرقم السري لبطاقة دفع عائدة للغير لعدم توفر القصد الجرمي لديه.

ج- العقوبة:

عاقب المشرع على جريمة الحصول دون وجه حق على بيانات أو أرقام بطاقة دفع باستخدام الأجهزة الحاسوبية أو الشبكة بعقوبة جنحوية الوصف وهي الحبس من ثلاثة أشهر إلى سنتين والغرامة من خمسمئة ألف إلى مليونين ونصف مليون ليرة سورية.

جريمة تزوير بطاقة الدفع

نصت الفقرة ب من المادة 22 من قانون مكافحة الجريمة المعلوماتية على ما يلي:

(يُعاقَب بالحبس من ثلاث إلى خمس سنوات والغرامة من خمسمئة ألف إلى مليونين ونصف مليون ليرة سورية، كل من:

1-قام بتزوير بطاقة دفع.

2-استعمل بطاقة دفع مزوّرة أو مسروقة أو مفقودة في الدفع أو سحب النقود.)

وقد عرف المشرع السوري التزوير في المادة /443/ من قانون العقوبات بأنه: (تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد أثباتها بصك أو مخطوط يحتج بهما، يمكن أن ينجم عنه ضرر مادي أو معنوي أو اجتماعي).

و قد عددت المادة /445/ عقوبات طرق التزوير المادية، كما حددت المادة /446/ عقوبات طرق التزوير المعنوية. وطرق التزوير المادية كما يستدل من اسمها، طرق أو وسائل

(58) د. عبد الفتاح بيومي حجازي، المرجع السابق، ص134.

مادية تترك أثراً مادياً على المحرر يمكن إدراكه إما بالحواس أو بالخبرة الفنية، وذلك بعكس طرق التزوير المعنوية التي لا تترك أثراً يدركه الحس، وبالتالي يصعب إثبات التزوير المعنوي لعدم وجود الأثر المادي. وعلى ذلك فإن طرق التزوير المادية من الممكن أن تتم أثناء تحرير المحرر أو بعد الانتهاء من تحريره، أما طرق التزوير المعنوية فلا تتحقق إلا أثناء تحرير المحرر [59].

وعلى ذلك سنعمد إلى دراسة الركن المادي والركن المعنوي لجريمة تزوير بطاقة الدفع في ضوء مفهوم التزوير المنصوص عليه في قانون العقوبات على التتالي:

<u>**أ- الركن المادي:**</u>

ينطوي الركن المادي في جريمة التزوير التقليدية على **تغيير الحقيقة** في محرر بإحدى **الطرق المحددة** قانوناً، ولتوافر هذا الركن يجب أنه يكون هناك محلاً يرد عليه فعل تغيير الحقيقة وهذا المحل هو **المحرر**، ونشاط جرمي يتمثل بتغيير الحقيقة بإحدى الطرق المحددة قانوناً ويندمج في هذا النشاط النتيجة الجرمية وهي أيضاً تغيير الحقيقة وعلاقة السببية بينهما. ثم يجب أن يترتب على التزوير عنصر الضرر، وهو شرط منفصل عن الركن المادي إلا أن غالبية الفقه الجزائي جرى على دراسته في إطار الركن المادي.

ويقصد بتغيير الحقيقة تحريفها أي استبدالها بغيرها، وذلك بإحلال أمر غير صحيح محل أمر صحيح، فإذا لم يكن هناك حقيقة مغيرة أو محرفة فلا يكون هناك تزوير، كمن يقلد توقيع شخص آخر على وثيقة بإذن صاحب الإمضاء ورضائه فلا يعد ذلك تزويراً لأن الحقيقة لم تتغير [60].

أما **المحرر فيقصد به** كل مكتوب يفصح عن مصدره ويتضمن وقائع أو بيانات تصلح لأن يحتج بها.

فالتزوير هو الكذب المكتوب، والمحل الذي يجب أن يرد عليه التزوير يجب أن يكون **مكتوباً**، أي أن يكون محرراً.

ويقصد بالكتابة في مجال التزوير العبارات الخطية أو العلامات أو الرموز التي تصلح لسرد واقعة أو للتعبير عن إرادة، أي تصلح لنقل المعنى من شخص لآخر، فلا تعد كتابة ولا تصلح محلاً لجريمة التزوير عدادات الكهرباء أو المياه أو الغاز، ولا الأختام المنسوبة لجهة عامة، ولا الرسومات أو لوحات الفن عموماً وإن كان يمكن أن يتوفر في تغيير الحقيقة لهذه

(59) د. علي عبد القادر القهوجي، المرجع السابق، ص 122.

(60) د. علي عبد القادر القهوجي، المرجع السابق، ص 116. وراجع أيضاً- د.محمود نجيب حسني، شرح قانون العقوبات-القسم الخاص، دار النهضة العربية-القاهرة، 1992،ص219.

الأشياء جرائم أخرى [61].

كما يخرج من مفهوم المحرر في جريمة التزوير التقليدي الاسطوانات أو أشرطة التسجيل أو الشريط الممغنط الذي سجلت عليه عبارات أياً كانت أهميتها، وبالتالي فإن تغيير الحقيقة الذي يطرأ على المعطيات والمعلومات المخزنة والمسجلة على اسطوانات أو شرائط ممغنطة لا يعد تزويراً، لأن هذه المعلومات المعالجة آلياً لا تعتبر محرراً، لأنه **لا يمكن مشاهدة** هذه المعلومات المسجلة كهرومغناطيسياً على هذه الشرائط عن طريق النظر [62].

إلا أنه وبعد صدور قانون الجريمة المعلوماتية أصبح يدخل في مفهوم المحرر تزوير المعلومات والبيانات المخزنة أو المسجلة على الأشرطة الممغنطة ولو لا يمكن مشاهدتها بالعين المجردة.

وبناءً على ذلك **فيقصد بتزوير بطاقة الدفع** كل تغيير في أحد بيانات البطاقة كرقمها أو اسم حاملها أو توقيعه، وكذلك البيانات الالكترونية المسجلة على الشريط الممغنط أو المخزنة ضمن البطاقة.

والواقع أن المشرع السوري لم يحدد طرق تزوير بطاقات الدفع، وبالتالي فيمكن أن يتم التزوير **بأي وسيلة كانت،** كالتلاعب بشريطها الممغنط أو ببياناتها مثل تاريخ الصلاحية واسم الحامل، أو تقليد البطاقة برمتها، أي صناعة بطاقة دفع على غرار بطاقة أخرى. كما يمكن أن يقع التزوير بوسيلة معنوية، كما لو انتحل الجاني شخصية صاحب الحساب في أحد المصارف، من أجل الحصول على بطاقة باسم صاحب الحساب الحقيقي[63].

ولا يكفي لقيام جريمة تزوير بطاقات الدفع أن يقع تغيير في الحقيقة في هذه البطاقات، بل لا بد لهذا التغيير من أن يسبب ضرراً للغير، وإن كان يكفي أن يكون هذا الضرر احتمالياً[64].

والضرر هو إهدار أو انتقاص لحق أو لمصلحة يقررها ويحميها القانون، وهو شرط لازم لقيام جريمة التزوير، فإذا انتفى انتفت الجريمة، ويتنوع الضرر إلى ضرر مادي ومعنوي، وضرر حال ومحتمل، وضرر فردي واجتماعي.

---

(61) د. علي عبد القادر القهوجي، المرجع السابق، ص 100 – وراجع أيضاً–العلامة رينيه غارو، موسوعة قانون العقوبات العام والخاص، ترجمة لين صلاح مطر، الجزء الخامس، منشورات الحلبي الحقوقية – بيروت، عام 2003 ص 92.

(62) د. جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الأئتمان الممغنطة، المرجع السابق، ص 117.

(63) د. نائلة قورة، المرجع السابق، ص 607.

(64) د.جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الأئتمان الممغنطة، المرجع السابق، ص132.

والضرر المادي هو الذي يصيب المجني عليه في ذمته المالية، والضرر المعنوي هو الذي ينال من شرف وكرامة واعتبار إنسان أو جماعة. أما الضرر الحال فهو الضرر الذي تحقق فعلاً، و أما الضرر المحتمل فهو الضرر الذي لم يقع بعد ولكن يحتمل وقوعه، ولا يشترط لقيام جريمة التزوير أن يكون الضرر قد وقع فعلاً، بل يكفي أن يكون وقوعه محتملاً (65).

أما الضرر الفردي أو الخاص فهو الضرر الذي يصيب فرداً أو هيئة أو جماعة خاصة سواء كان مادياً أو أدبياً حالاً أو محتملاً.

أما الضرر الاجتماعي أو العام فهو الذي يصيب المجتمع ككل أو الجسم الاجتماعي أي يمس الصالح العام، ومن أمثلة الضرر الاجتماعي المادي تزوير إيصال بسداد ضريبة، ومن أمثلة الضرر الاجتماعي المعنوي، دخول شخص إلى الامتحان باسم شخص آخر ليحصل على شهادة باسم الأخير (66).

وبالنسبة لتزوير بطاقات الدفع، فإن الضرر الذي يترتب عليه هو **ضرر مادي محتمل** بالنسبة لحامل البطاقة، بالإضافة إلى **ضرر اجتماعي مادي ومعنوي** نظراً لما يصيب المجتمع من اهتزاز بالثقة في المعاملات (67).

ب: الركن المعنوي:

جريمة التزوير جريمة مقصودة يتخذ فيها الركن المعنوي صورة القصد الجرمي، والقصد الجرمي الواجب توافره لقيام جريمة التزوير ليس فقط القصد العام وإنما يجب أن يضاف إليه القصد الخاص.

والقصد العام اللازم لقيام جريمة التزوير هو العلم والإرادة، أي العلم بأركان الجريمة وعناصرها، والإرادة التي تتجه إلى السلوك الجرمي ونتيجته.

أما **القصد الخاص** الذي يجب توافره لتحقق القصد الجرمي في جريمة التزوير هو نية إحداث ضرر مادي أو معنوي أو اجتماعي بالمعنى الذي سبق الإشارة إليه في شرح عنصر الضرر.

---

(65) نقض سوري رقم /638/ أساس 492 تاريخ 1988/7/23، منشور في مجموعة أحكام النقض في قانون العقوبات والقوانين المتممة، إعداد عبد القادر جار الله الجزء الأول الطبعة الأولى، المكتبة القانونية دمشق، عام 2001، ص513.

(66) د. علي عبد القادر القهوجي، المرجع السابق ص144.

(67) د. جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة،المرجع السابق ص128.

جريمة استعمال بطاقة دفع مزورة أو مسروقة أو مفقودة

عاقب المشرع في الفقرة ب من المادة 22 من قانون مكافحة الجريمة المعلوماتية على استعمال بطاقة دفع مزوّرة أو مسروقة أو مفقودة بالحبس من ثلاث إلى خمس سنوات والغرامة من خمسمئة ألف إلى مليونين ونصف مليون ليرة سورية.

وسنتناول الركن المادي والركن المعنوي لهذه الجريمة فيما يلي:

أ- الركن المادي:

تفترض جريمة استعمال بطاقة الدفع المزورة، سبق وجود بطاقة مزورة، وقد جعل المشرع السوري من جريمة استعمال البطاقات المزورة جريمة مستقلة عن جريمة تزويرها، وعليه فلا يشترط أن يكون مستعمل البطاقة هو من قام بتزويرها، بل يكفي أن يكون عالماً بأن البطاقة التي يقوم باستعمالها مقلدة أو مزورة.

وجوهر الركن المادي هنا هو **فعل الاستعمال** ويقصد به التمسك بالبطاقة المزورة أو الاحتجاج بها على أساس أنها صحيحة، وهذا يعني أن يصدر عن الجاني عمل إيجابي في معرض استعماله لهذه البطاقة، فمجرد وجود البطاقة المزورة في حيازة شخص دون إبرازها أو تقديمها لا يقوم به فعل الاستعمال، وبالتالي يجب لقيام جريمة الاستعمال أن يقوم الجاني بإبراز البطاقة والاحتجاج بها على أنها صحيحة[68].

ويترتب على استقلال جريمة التزوير عن جريمة استعمال المزور، أن فعل التزوير معاقب عليه ولو لم يستعمل الجاني البطاقة المزورة، كما لو قام الجاني بتزوير بطاقة دفع ثم باعها للغير، فإنه يعاقب على التزوير ولو أصبح استعمال البطاقة المزورة مستحيلاً نتيجة إدراجها على قائمة البطاقات المزورة.

ويترتب أيضاً على قاعدة الاستقلال، أنه من الممكن أن تترتب مسؤولية مستعمل المزور دون أن تترتب مسؤولية المزور، كما لو قام شخص بتقليد بطاقة دفع ووضعها على واجهة محله كنوع من الدعاية، فانتزعها شخص آخر واستعملها وهو يعلم بتزويرها، فهنا تقوم جريمة استعمال المزور في حق مستعمل البطاقة رغم عدم قيامها في حق المزور لانتفاء القصد الجرمي.[69]

---

(68) راجع في معنى استعمال المحرر د.علي عبد القادر القهوجي، المرجع السابق ص183. د. نائلة قورة، المرجع السابق، ص 608.

(69) د. جميل عبد الباقي الصغير، الحماية الجنائية والمدنية لبطاقات الأئتمان الممغنطة، المرجع السابق، ص 138.

وقد ساوى المشرع من حيث العقاب بين استعمال البطاقة المزورة واستعمال البطاقة المسروقة أو المفقودة، فقد يحدث أن تتم سرقة البطاقة أو تتعرض للضياع ومعها الرقم السري، وغالباً ما يقوم المصرف بإلزام عميله في حالة السرقة أو الضياع بأن يبلغ عن الحادثة فوراً لإيقاف العمل بالبطاقة.

ومما لا شك فيه، فإن مسؤولية الحامل الشرعي تنتفي من اللحظة التي يتم فيها الإبلاغ عن سرقة أو فقدان البيانات السرية لبطاقة الدفع، فلا يُسأل عن استعمال البطاقة احتيالياً. ويجب على المصرف المصدر للبطاقة أن يوقف التعامل بها فوراً، وإلا كان مسؤولاً عن العمليات المالية التي تتم بواسطتها[(70)].

وحتى يتخلص المصرف من المشاكل المتعلقة بموعد الإبلاغ، فقد تم إنشاء نظام تأمين للتعويض عن سرقة البطاقات أو ضياعها إذا ما تم استعمالها في السحب أو الوفاء، ويحدد المبلغ القابل للتعويض في العقد المبرم بين المصرف والعميل. كما تمت برمجة أجهزة التوزيع الآلي للنقود على افتراض وجود محاولات يقوم بها الجاني لتجربة بعض الأرقام حتى يتوصل إلى الرقم السري، فبعد إجراء ثلاث محاولات مثلاً، يقوم الجهاز بسحب البطاقة ولا يعيدها له، فإذا كان هو حاملها الشرعي فيستطيع استردادها عن طريق المصرف المصدر لها[(71)].

ولم يشترط المشرع في جريمة الاستعمال أن يحصل الجاني على مال المجني عليه نتيجة هذا الاستعمال، وبالتالي فتتحقق هذه الجريمة ولو كان حساب المجني عليه فارغاً مثلاً، أما إذا استطاع الجاني أن يستولي على مال المجني عليه فنكون هنا أما حالة اجتماع جرائم معنوي لأن فعله ينطبق عليه وصف الاستعمال ووصف الاحتيال.

ب–الركن المعنوي:

جريمة استعمال بطاقة مزورة أو مسروقة أو مفقودة، جريمة مقصودة، ومن ثم تتطلب لقيام الركن المعنوي توفر القصد الجرمي العام بعنصريه العلم والإرادة، وعليه يجب أن يكون المدعى عليه عالماً بأن البطاقة مزورة أو مسروقة أو مفقودة، وأن تتجه إرادته إلى إبرازها واستعمالها، وبالتالي فإن جريمة الاستعمال تنتفي إذا ثبت أن المدعى عليه كان يجهل بأن البطاقة مزورة أو مسروقة أو مفقودة.

وفي إحدى القضايا التي عرضت على قضائنا السوري، أنه في عام 2011 قام مجموعة من الأشخاص بتزوير بطاقات الدفع واستعمالها بسحب النقود، وذلك عن طريق قيام أحد أفراد

(70) المحامي محمد أمين الشوابكة: المرجع السابق، ص199.

(71) د. أحمد حسام طه تمام: المرجع السابق، ص535.

هذه العصابة بالوقوف أمام أجهزة الصراف الآلي وانتحاله صفة موظف مسؤول عن أمن الصراف، وقيامه بطلب البطاقات من أصحابها لفحصها على جهاز إلكتروني موجود في حوزته للتأكد من سلامتها، وبعد قيام المجني عليهم بتسليمه بطاقاتهم يقوم بتمريرها على جهاز ماسح إلكتروني لنسخ بياناتها ومعلوماتها، ثم يتم تزوير بطاقات تحمل ذات البيانات الحقيقية، و من ثم يتم سحب مبالغ من أجهزة الصراف الآلي داخل القطر وخارجه، وقد تم ملاحقة هذه العصابة بجريمة الاحتيال وفق المادة 641 عقوبات كونها ارتكبت قبل صدور قانون مكافحة الجريمة المعلوماتية، وصدر قرار بالظن بهذه الجريمة من قاضي التحقيق المختص(72).

وفي قضية أخرى عرضت على قضائنا أيضاً، أنه في عام 2009 قام مستخدم بإحدى المصارف بسرقة بطاقة دفع مع رقمها السري أثناء عمله بتنظيف إحدى الغرف، ثم قام بسحب مبالغ مالية وصلت إلى مائتين وثمانية وعشرون ألف ليرة سورية من حساب هذه البطاقة المسروقة، وقد تم اكتشاف هذه الجريمة بعد قيام صاحبة البطاقة بتقديم شكوى تتضمن وجود نقص في رصيدها، حيث تمت مراجعة كاميرات المراقبة الموجودة على أجهزة الصراف، وتم التعرف على المستخدم الذي استخدم هذه البطاقة والذي اعترف بسرقتها أيضاً. وقد حُركت الدعوى العامة بحق المستخدم بجرم السرقة من مكان الاستخدام وجرم الاحتيال(73).

تاسعاً: جريمة انتهاك الحياة الخاصة:

نصت المادة 23 من قانون مكافحة الجريمة المعلوماتية على ما يلي:

(يُعاقَب بالحبس من شهر إلى ستة أشهر والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية، كل من نشر عن طريق الشبكة معلومات تنتهك خصوصية أي شخص دون رضاه، حتى ولو كانت تلك المعلومات صحيحة.)

وسنتناول الركن المادي والركن المعنوي لهذه الجريمة فيما يلي:

أ- الركن المادي:

عرف المشرع السوري في المادة الأولى من قانون مكافحة الجريمة المعلوماتية **الخصوصية** بأنها: **(**حق الفرد في حماية أسراره الشخصية والملاصقة للشخصية والعائلية، ومراسلاته، وسمعته وحرمة منزله، وملكيته الخاصة، وفي عدم اختراقها أو كشفها دون موافقته**)**.

(72) ضبط إدارة الأمن الجنائي رقم 788 تاريخ 2011/9/27 وقرار السيد قاضي التحقيق الخامس بدمشق بالدعوى أساس 1627 قرار رقم 774 تاريخ 2011/10/23.

(73) ضبط قسم شرطة عرنوس رقم 791 تاريخ 2009/3/23، والدعوى مازالت منظورة أمام محكمة بداية الجزاء العاشرة بدمشق برقم أساس 159 لعام 2012.

فالخصوصية ترتبط بالشخصية الإنسانية، وهي عبارة عن مجموعة من الوقائع والعلاقات التي تساهم في تحديد هذه الشخصية، وتضم كافة العلاقات ذات الطابع الشخصي للإنسان، مثل الحياة العاطفية، والحالة الصحية، والحالة المدنية، ومحل الإقامة، والاتجاه السياسي... إلخ. فمثل هذه المعلومات يجب عدم التعرض لها أو المساس بها من قبل الغير، ما لم يكن هناك قبول صريح أو ضمني من صاحبها. فالخصوصية ذات قيمة إنسانية، وهي بذلك لا تشمل الأسرار الشخصية فقط، وإنما تمتد إلى الأمور الخاصة التي قد لا تكون سرية، ومع ذلك يحظر على الغير التدخل فيها[74].

أما النشاط الجرمي لهذه الجريمة فيتمثل بفعل النشر على الشبكة للمعلومات التي تتعلق بالخصوصية، ويشترط أن يكون النشر دون رضاء صاحب هذه المعلومات، ولا عبرة لكون هذه المعلومات صحيحة أم لا، وعلى ذلك فمن ينشر على موقع إلكتروني العلاقة العاطفية لشخص ما دون رضائه يسأل عن جريمة انتهاك حرمة الحياة الخاصة.

و قد يكون الفاعل قد حصل على هذه المعلومات من صاحبها برضاه إلا أنه لم يخوله نشرها، وغني عن البيان أنه في حالة نشر معلومات غير صحيحة تتعلق بخصوصية شخص ما فإن ذلك قد يشكل جريمة الذم عبر الشبكة.

ب- الركن المعنوي:

جريمة انتهاك حرمة الحياة الخاصة جريمة مقصودة تتطلب القصد الجرمي العام بعنصريه العلم والإرادة، فيجب أن يعلم الجاني بطبيعة المعلومات المتعلقة بالخصوصية، وأن صاحب هذه المعلومات لم يأذن له أو يخوله بنشرها، كما يجب أن تتجه إرادته إلى هذا النشر عبر الشبكة رغم عدم رضاء صاحب هذه المعلومات.

ج- العقوبة:

عاقب المشرع على جريمة انتهاك حرمة الحياة الخاصة بعقوبة جنحوية الوصف وهي الحبس من شهر إلى ستة أشهر والغرامة من مئة ألف إلى خمسمائة ألف ليرة سورية.

---

(74) د. عمر بن يونس، الجرائم الناشئة عن استخدام الانترنت، المرجع السابق، ص593-594.

الأحكام العامة لجرائم المعلوماتية

تضمن الفصل الخامس من قانون مكافحة الجريمة المعلوماتية الأحكام العامة المتعلقة بهذا القانون، كالظروف المشددة التي تشمل جميع نصوصه التجريمية، والشروع، والعلنية، والمصادرة وغيرها من القواعد العامة المتعلقة بالجرائم التقليدية والنواحي الإجرائية.

وستناول في هذا الجزء القواعد المتعلقة بظروف التشديد والشروع والعلنية والمصادرة على التتالي:

أولاً: ظروف التشديد:

نصت المادة 30 من قانون مكافحة الجريمة المعلوماتية على ما يلي:

(تشدّد العقوبات، وفق القواعد العامة للتشديد المنصوص عليها في قانون العقوبات النافذ، في الحالات التالية:

1) إذا كان موضوع الجريمة يمسّ الدولة أو السلامة العامة.

2) إذا جرى ارتكاب الجريمة بواسطة عصابة منظّمة.

3) إذا وقعت الجريمة على قاصر أو من في حكمه.

4) إذا استغلّ مرتكب الجريمة عمله الوظيفي لارتكاب الجريمة.)

وعليه فقد حدد المشرع أربعة ظروف تؤدي إلى تشديد العقوبة وفق المادة 247 من قانون العقوبات وهذه الظروف هي:

أ-**إذا كان موضوع الجريمة يمس الدولة أو السلامة العامة:**

ويتحقق ظرف التشديد هذا عندما يكون محل الجريمة يمس الأجهزة الحكومية كالوزارات والإدارات والشركات والمؤسسات والجهات الأخرى التابعة للقطاع العام والمشترك، ويستوي هنا أن يكون محل الجريمة **المعلومات** أو **الأموال** العائدة للدولة، وتشمل المعلومات مختلف أنواعها سواء أكانت معلومات تمس أمن الدولة أو لا، كالمعلومات المتعلقة بشؤون الموظفين أو المعلومات المتعلقة بموارد الدولة وغير ذلك من المعلومات. كما لو قام الجاني بالدخول بطريقة غير مشروعة إلى المعلومات المخزنة في حواسيب إحدى الوزارات سواء تم الدخول بطريقة مباشرة أم غير مباشرة، وقام بنسخ هذه المعلومات أو إتلافها أو تغييرها.

كما يتحقق ظرف التشديد إذا كان محل الجريمة **أموال** عائدة للدولة سواء أكانت هذه الأموال منقولة أم غير منقولة، أم كانت عائدة برمتها إلى القطاع العام أو المشترك، كما لو قام

الجاني باختراق موقع إلكتروني عائد لأحد مصارف الدولة وقام بتحويل الأموال لحسابه بطريقة غير مشروعة.

و يتحقق ظروف التشديد أيضاً إذا كان محل الجريمة **يمس السلامة العامة** والحقيقة أن مفهوم السلامة العامة من الأتساع بمكان بحيث يصعب تحديده تحديداً دقيقاً، فالمشرع لم يقم بتحديد معنى هذه العبارة، ولم تقم التعليمات التنفيذية لهذا القانون بذلك أيضاً. ويمكن أن **نحدد مفهوم السلامة العامة** هنا في الحالات التي ينتج عن الجريمة ضرر بالصحة العامة أو بفئة معينة من الناس، كما لو قام الجاني باختراق حواسيب معمل للأدوية عن طريق الإنترنت، ثم قام بالتلاعب بكميات المواد الدوائية الداخلة في تصنيع الأدوية، الأمر الذي أدى إلى حدوث أضرار صحية عند مستخدمي هذه الأدوية. ففي هذه الحالة نكون أمام جريمة إيذاء مقصود مع ظرفين للتشديد، الأول هو ظرف التشديد المنصوص عليه بالفقرة ب من المادة 28 من قانون مكافحة الجريمة المعلوماتية والذي يضاعف الحد الأدنى لعقوبة الجريمة المنصوص عليها في القوانين الجزائية إذا ارتكبت باستخدام الشبكة كالإنترنت، أما ظرف التشديد الثاني فهو المنصوص عليه في المادة 30 لأن الجريمة أدت إلى الأضرار بالسلامة العامة.

ب- ارتكاب الجريمة بواسطة عصابة منظمة:

عرف المشرع في المادة الأولى من قانون مكافحة الجريمة المعلوماتية **العصابة المنظمة** بأنها: (جماعة أشخاص أو فعّاليات، عادة ما تكون ذات تنظيم مركزي، تهدف إلى ممارسة الأنشطة الإجرامية، سواء على الصعيد الوطني أو الإقليمي أو الدولي).

والواقع أن المشرع لم يحدد في هذا التعريف الحد الأدنى المطلوب قانوناً لأفراد هذه العصابة، وفي تقديرنا أن الحد الأدنى لأفراد العصابة المنظمة يجب أن يكون ثلاثة أشخاص فأكثر، وذلك تماشياً مع سياسة المشرع السوري في المادة 326 عقوبات المتعلقة بجمعيات الأشرار، وتعريف الجماعة الإجرامية في قانون مكافحة الاتجار بالأشخاص رقم 3 لعام 2010، حيث اشترط المشرع في كلا الحالتين أن تتكون الجماعة من ثلاثة أشخاص فأكثر.

وبناءً على ذلك فيتحقق ظرف التشديد المذكور، إذا تم تكوين جماعة من ثلاثة أشخاص فأكثر، ذات تنظيم مركزي، بهدف ارتكاب إحدى الجرائم المنصوص عليها في قانون مكافحة الجريمة المعلوماتية، ويقصد بالتنظيم المركزي أن يكون هناك توزيع لدور كل فرد من أفراد الجماعة في ارتكاب الجرائم، سواء أكانت هذه الجماعة تعمل على الصعيد الوطني أو الإقليمي أو الدولي.

جـ – إذا وقعت الجريمة على قاصر أو من في حكمه:

ويقصد بالقاصر كل ذكر أو أنثى لم يتم الثامنة عشر من عمره، أما من هو في حكم القاصر فهم فاقدو وناقصو الأهلية كالمجنون والمعتوه والسفيه وذو الغفلة، وعلة التشديد في هذه الحالات هو حاجة هؤلاء للحماية القانونية أكثر من غيرهم بسبب ضعفهم وعدم قدرتهم على حماية أنفسهم، ومثال ذلك الأفلام والصور الخلاعية الموجهة للقاصرين على الانترنت.

د– إذا استغل مرتكب الجريمة عمله الوظيفي لارتكاب الجريمة:

ويتحقق ظرف التشديد هنا عندما يقوم العامل في إحدى الجهات العامة أو الخاصة بارتكاب إحدى جرائم المعلوماتية مستغلاً وضعه الوظيفي، أي عندما تسهل الوظيفة ارتكاب الجريمة، كما لو قام أحد العاملين بالدخول إلى الأجهزة الحاسوبية لشركة ما ونسخ المعلومات دون أن يكون مصرح له بذلك.

ثانياً: الشــروع:

نصت المادة 31 من قانون الجريمة المعلوماتية على ما يلي:

(يُعاقب على الشروع في الجنح المنصوص عليها في هذا القانون، وفق الأحكام الواردة في قانون العقوبات النافذ.)

والشروع –وفقاً للقواعد العامة– هو كل محاولة لارتكاب جناية أو جنحة (معاقب على الشروع فيها) بدأت بأفعال ترمي مباشرة إلى اقترافها، تعتبر كالجريمة نفسها إذا لم يحل دون إتمامها سوى ظروف خارجة عن إرادة الفاعل[75].

فالشروع هو جريمة بدأت فيها الأفعال التنفيذية إلا أن النتيجة الجرمية لم تتحقق لظروف خارجة عن إرادة الفاعل. والمعيار الذي أخذ به المشرع السوري للتمييز بين الأفعال التحضيرية والأفعال التنفيذية، هو المعيار الشخصي الذي ينظر إلى مقدار الخطورة التي وصل إليها الجاني من خلال أفعاله، وهو المعيار الذي يحقق للمجتمع حماية أكبر. أما المعيار المادي فهو ضيق؛ لأنه لا يعاقب الفاعل على أفعاله إلا إذا كانت داخلة ضمن الركن المادي للجريمة أو لظرف مشدد لها[76].

والأصل أنه إذا وقف نشاط الفاعل عند العمل التحضيري فلا عقاب عليه، إلا إذا كانت الأفعال التي قام بها تشكل جرائم بحد ذاتها.

---

(75) راجع المواد 199– 200– 201– 202 عقوبات.

(76) د. عبود السراج: شرح قانون العقوبات، القسم العام، منشورات جامعة دمشق،عام 2007، ص315.

والشروع نوعان: شروع تام، وفيه يقوم الجاني بجميع الأفعال التنفيذية إلا أن النتيجة الجرمية لا تتحقق لظروف خارجة عن إرادته. ويطلق على هذا الشروع أيضاً اسم الجريمة الخائبة. أما النوع الثاني فهو **الشروع الناقص**، وفيه لا يكتمل النشاط الجرمي، وتتوقف الجريمة في مراحلها الأولى لظروف خارجة عن إرادة الفاعل. ويطلق على هذا الشروع اسم الجريمة الموقوفة.

والشروع بنوعيه يمكن تصوره في جرائم المعلوماتية، فمن يقوم باختراق نظام معلوماتي لأحد المصارف عن طريق الإنترنت، ويقوم بإدخال البيانات اللازمة لإجراء التحويلات المالية غير المشروعة، ثم لا تتحقق النتيجة الجرمية المتمثلة بتحويل النقود، نتيجة وجود خطأ في إدخال بعض البيانات، فإن نشاط الفاعل يشكل هنا شروعاً تاماً في الاحتيال.

وقد يقف نشاط الفاعل عند حد الشروع الناقص، كما لو تم إلقاء القبض على أحد الهكرة أثناء وجوده في أحد مقاهي الإنترنت، وهو يقوم باختراق إحدى شبكات المصارف، بغية إجراء تحويلات غير مشروعة.

ثالثاً: العلنية على الشبكات المعلوماتية:

نصت المادة 32 من قانون مكافحة الجريمة المعلوماتية على ما يلي:

(تعدّ الشبكة من وسائل العلنية المنصوص عليها في قانون العقوبات والقوانين الجزائية النافذة.)

وقد حدد المشرع وسائل العلنية في قانون العقوبات بالمادة 208 التي نصت على ما يلي:

(تعد وسائل للعلنية:

1 . الأعمال والحركات إذا حصلت في محل عام أو مكان مباح للجمهور أو معرض للأنظار أو شاهدها بسبب خطأ الفاعل من لا دخل له بالفعل.

2 . الكلام أو الصراخ سواء جهر بهما أو نقلاً بالوسائل الآلية بحيث يسمعهما في كلا الحالين من لا دخل له بالفعل.

3 . الكتابة والرسوم والصور اليدوية والشمسية والأفلام والشارات والتصاوير على اختلافها إذا عرضت في محل عام أو مكان مباح للجمهور أو معرض للأنظار أو بيعت أو عرضت للبيع أو وزعت على شخص أو أكثر.)

وبناء على ذلك فقد جعل المشرع من **الشبكة** كالانترنت والشبكات الداخلية وشبكات الهاتف النقال وغيرها من الشبكات، وسيلة من وسائل العلنية، **بمعنى أنها أصبحت تنزل منزلة المحل العام أو المكان المباح للجمهور**، فالعلنية تتحقق في المعلومات التي توضع في متناول عامة الجمهور أو فئة منه على موقع إلكتروني، والتي يمكن لأي فرد الوصول إليها. ولا يدخل في مفهوم العلنية المراسلات ذات الطابع الشخصي التي تتم عبر البريد الإلكتروني، أو في المحادثات الشخصية على الشبكة.

والحقيقة أن هناك طائفة من الجرائم التقليدية التي اشترط المشرع فيها أن ترتكب بوسيلة علنية، كجريمتي الذم والقدح العلني المنصوص عليهما بالمادتين 568 و 570 عقوبات، وجريمتي الذم والقدح العلني الموجه إلى موظف المنصوص عليهما بالمادتين 376 و 378 عقوبات، وجريمة تحقير علم الدولة بشكل علني المنصوص عليها بالمادة 374 عقوبات، وغير ذلك من الجرائم. فشرط العلنية المطلوب يتحقق في جميع هذه الجرائم إذا ارتكبت على الشبكة.

رابعاً: المصادرة:

نصت المادة 34 من قانون مكافحة الجريمة المعلوماتية على ما يلي:

(أ- مع عدم الإخلال بحقوق الغير الحسني النية، تحكم المحكمة بمصادرة الأجهزة والبرمجيات الحاسوبية، أو أي وسائل أخرى مستخدمة في ارتكاب أيٍ من الجرائم المنصوص عليها في هذا القانون.

ب- و يجوز أيضاً الحكم بوقف أو إغلاق الموقع الإلكتروني المستخدم في ارتكاب أيٍ من الجرائم المنصوص عليها في هذا القانون، أو أي منظومة مشابهة، إذا كانت الجريمة قد ارتكبت بعلم صاحب هذا الموقع أو المنظومة.)

و **المصادرة** هنا هي مصادرة عينية(77) و هي عقوبة مالية إضافية، تنزع بموجبها ملكية شيء للمحكوم عليه جبراً، ومن غير مقابل ليصبح ملكاً للدولة. وقد جعل المشرع من مصادرة الأجهزة والبرمجيات الحاسوبية، أو الوسائل الأخرى المستخدمة في ارتكاب أيٍ من الجرائم المنصوص عليها في قانون مكافحة الجريمة المعلوماتية. عقوبة إضافية وجوبية، أي يجب على المحكمة أن تحكم بها في حكمها النهائي. أما الحكم بوقف أو إغلاق الموقع الإلكتروني المستخدم في ارتكاب أيٍ من الجرائم المنصوص عليها في قانون مكافحة الجريمة المعلوماتية، أو أي منظومة مشابهة، إذا كانت الجريمة قد ارتكبت بعلم صاحب هذا الموقع أو المنظومة. فهو

---

(77) راجع المادة 69 من قانون العقوبات.

أمر جوازي يعود تقديره إلى المحكمة، وهو من قبيل تدابير الاحتراز العينية التي تهدف إلى علاج المجرم، ومنعه من العودة إلى ارتكاب الجريمة، وحماية المجتمع من خطره.

تمارين:

اختر الإجابة الصحيحة:

في جريمة اعتراض المعلومات:

1) يجب الدخول إلى حاسوب الغير ونسخ المعلومات.
2) يجب الدخول إلى حاسوب الغير وتعديل المعلومات.
3) يجب الدخول إلى حاسوب الغير وإتلاف المعلومات.
4) يجب التنصت على المعلومات أثناء تبادلها.

الإجابة الصحيحة رقم 4

الأحكام الموضوعية للجريمة المعلوماتية

الوحدة التعليمية الثالثة

2- الجرائم التقليدية

الكلمات المفتاحية:

الجرائم التقليدية والشبكة- تطبيق النصوص الجزائية-ارتكاب الجرائم التقليدية باستخدام الشبكة- الاعمال الدعائية والتحريض على ارتكاب الجرائم.

المخلص:

تتضمن هذه الوحدة التعليمية شرح للقواعد التي تتعلق بتطبيق النصوص الجزائية ، والعقوبة الفروضة على ارتكاب الجرائم التقليدية باستخدام الشبكة، والجرائم التي تقع على الاجهزة الحاسوبية بهدف التاثير على عملها . والأعمال الدعائية والتحريض على ارتكاب الجرائم التقليدية عبر الشبكة.

الأهداف التعليمية:

تهدف هذه الوحدة التعليمة إلى تعليم الطالب كيفية تشديد العقوبة عندما ترتكب الجرائم التقليدية باستخدام الشبكة بشرط أن يكون للشبكة دور ايجابي بارتكاب الجريمة مع ضرب الأمثلة على ذلك. والعقوبة المفروضة على التحريض على الجرائم التقليدية عندما ترتكب على الشبكة.

أفرز عصر المعلومات رغم إيجابيته العديد من السلبيات، حيث استخدمت الشبكات لارتكاب الجرائم التقليدية، وهي الجرائم التي كانت موجودة قبل هذا العصر التقني، فراحت تبدو وكأنها جرائم جديدة، كما استخدمت الشبكة لترويج هذه الجرائم والتحريض على ارتكابها.

وبناءً على ذلك سندرس:

- الجرائم التقليدية والشبكة
- الأعمال الدعائية والتحريض على ارتكاب الجرائم

الجرائم التقليدية والشبكة

وضع المشرع القواعد المتعلقة بارتكاب الجرائم التقليدية باستخدام الشبكة، وبكيفية تطبيق القوانين الجزائية في المادة 28 من قانون مكافحة الجريمة المعلوماتية التي نصت على ما يلي:

(أ- إذا انطبق نصّ في القوانين الجزائية النافذة على إحدى الجرائم المنصوص عليها في هذا القانون، تُطبَّق العقوبة التي هي أشد.

ب- يُضاعف الحدّ الأدنى للعقوبة المقرّرة لأي من الجرائم المنصوص عليها في القوانين الجزائية النافذة الأخرى في إحدى الحالتين التاليتين:

1- إذا ارتُكبت الجريمة باستخدام الشبكة أو وقعت على الشبكة.

2- إذا وقعت الجريمة على جهاز حاسوبي أو منظومة معلوماتية، بقصد التأثير على عملها، أو على المعلومات أو البيانات المخزّنة عليها).

و سنتناول الأحكام التي جاءت بها هذه المادة على التتالي:

أولاً: تطبيق النصوص الجزائية:

أشارت الفقرة (أ) من المادة 28 من قانون مكافحة الجريمة المعلوماتية إلى أنه إذا انطبق نص في القوانين الجزائية النافذة على إحدى الجرائم المنصوص عليها في قانون مكافحة الجريمة المعلوماتية فيجب تطبيق النص ذو العقوبة الأشد، والغاية من هذا النص واضحة، وهي رغبة المشرع في تطبيق العقوبة الأشد في حالة انطباق نصين على واقعة ما تتعلق بجرائم المعلوماتية، والمثال على ذلك هو أن المادة 29 من قانون مكافحة الجريمة المعلوماتية تعاقب بالحبس من ستة أشهر إلى ثلاث سنوات والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية على كل من يقوم بالترويج لأي جريمة باستخدام الشبكة، وقد جاءت المادة 8 من قانون مكافحة الإرهاب الصادر بالقانون رقم 19 تاريخ 2012/7/2 لتعاقب بالأشغال الشاقة المؤقتة جريمة ترويج الأعمال الإرهابية المرتكبة على موقع إلكتروني، ففي هذه الحالة يجب على المحكمة أن تطبق النص ذو العقوبة الأشد وهو نص المادة 8 من قانون مكافحة الإرهاب.

ثانياً: ارتكاب الجرائم التقليدية باستخدام الشبكة أو عليها:

نصت الفقرة (ب) من المادة 28 على ما يلي: (يُضاعف الحدّ الأدنى للعقوبة المقرّرة لأي من الجرائم المنصوص عليها في القوانين الجزائية النافذة الأخرى في إحدى الحالتين التاليتين:

1- إذا ارتُكبت الجريمة باستخدام الشبكة أو وقعت على الشبكة.

2- إذا وقعت الجريمة على جهاز حاسوبي أو منظومة معلوماتية، بقصد التأثير على عملها، أو على المعلومات أو البيانات المخزّنة عليها).

و قد تستخدم الشبكة وخاصة الانترنت لارتكاب الجرائم التقليدية المنصوص عليها في التشريعات النافذة، ومن أمثلة هذه الجرائم :

- جريمة الذم المنصوص عليها بالمادة 568 من قانون العقوبات.

- جريمة القدح المنصوص عليها بالمادة 570 من قانون العقوبات.

- جريمة التعرض للآداب العامة المنصوص عليها بالمادة 517 من قانون العقوبات.

- جريمة التعرض للأخلاق العامة المنصوص عليها بالمادة 518 من قانون العقوبات.

- جريمة توزيع الصور والأفلام المخلة بالحياء المنصوص عليها بالمادة 519 من قانون العقوبات.

- جريمة توجيه الكلام المخل بالحشمة المنصوص عليها بالمادة 506 من قانون العقوبات.

- جريمة التهديد بجناية مثل القتل المنصوص عليها بالمادة 561 من قانون العقوبات.

- جريمة إثارة النعرات المذهبية التي ترتكب بالكتابة أو الخطاب المنصوص عليها بالمادة 307 من قانون العقوبات.

- جريمة الاستحصال على أسرار تتعلق بأمن الدولة المنصوص عليها بالمادة 272 من قانون العقوبات.

- جريمة إذاعة أنباء كاذبة في الخارج من شأنها أن تنال من هيبة الدولة المنصوص عليها بالمادة 287 من قانون العقوبات.

فجميع هذه الجرائم وغيرها يمكن أن ترتكب باستخدام الشبكة وخاصة الانترنت، والحقيقة أنه لابد من أن يكون لاستخدام الشبكة **دور إيجابي** في ارتكاب الجريمة، كأن يرتكب النشاط الجرمي بواسطة الشبكة أو أن يكون للشبكة دور على قدر من الأهمية في ارتكاب الجريمة، كإرسال عبارات التهديد بالقتل إلى المجني عليه عبر البريد الإلكتروني، أو نشر العبارات التي تثير النعرات الطائفية على موقع إلكتروني، أما إذا كان دور الشبكة ثانوياً، فلا يمكن القول بأن الجريمة ارتكبت باستخدام الشبكة، كاستخدام الشبكة لمجرد التواصل، والمثال على ذلك إرسال

بريد إلكتروني من الجاني إلى المجني عليه لترتيب لقاء بينهما في مكان ما، ثم قيام الجاني بقتل المجني عليه، أو إجراء اتصال بينهما عبر الشبكة لتحديد مكان اللقاء، ففي مثل هذه الحالة لا تعتبر جريمة القتل بأنها ارتكبت باستخدام الشبكة، لأن الشبكة لم يكن لها أي دور إيجابي في ارتكاب الجريمة.

ومن الأمثلة الواقعية على الدور الإيجابي للانترنت في جرائم القتل، أن رجلاً قتل زوجته التي كانت موضوعة تحت المراقبة في المستشفى، بأن دخل عبر الانترنت إلى شبكة المعلومات الخاصة بالمستشفى، ثم قام بتغيير المعلومات الطبية الخاصة بالمجني عليها المريضة[1] .

وغني عن البيان فإن **الركن المعنوي المطلوب في الجرائم التقليدية** التي ترتكب في العالم المادي لا يختلف فيما إذا ارتكبت هذه الجرائم عبر الشبكة، فالعلاقة الذهنية النفسية التي يكون عليها الفاعل ساعة ارتكاب الجريمة وهي جوهر الركن المعنوي لا تتأثر لكون الجريمة ارتكبت عبر الشبكة، فجميع القواعد المتعلقة بالقصد الجرمي وعناصره وأنواعه، والخطأ وعناصره وصوره يمكن تطبيقها على الركن المعنوي في الجرائم التقليدية التي ترتكب عبر الشبكة.

وفي جرائم المعلوماتية عموماً يمكن إثبات القصد الجرمي من خلال القرائن، فتفتيش حاسوب المشتبه به مثلاً، ومعرفة المواقع التي قام بتصفحها والأشخاص الذين اتصل بهم، قد يفيد في إثبات قصده الجرمي. ومن الوقائع الحقيقية التي تمّ فيها اكتشاف نية المدعى عليه في إحدى جرائم القتل، بأنه لدى تفتيش حاسوب المدعى عليه تبين بأنه كان يبحث عن مصطلحات مثل "قتل، خنق، وفيات، حادث" قبل قيامه بقتل زوجته، فبفضل عملية البحث هذه تم إثبات نية العمد لديه، ورفع مستوى الجريمة إلى القتل من الدرجة الأولى[2].

ثالثاً: ارتكاب الجريمة على جهاز حاسوبي أو منظومة معلوماتية بقصد التأثير على عملها أو على المعلومات أو البيانات المخزنة عليها:

والحقيقة أن غاية المشرع من هذه الفقرة هي وضع نص عقابي **احتياطي** يطال مختلف الجرائم التي تهدف إلى التأثير على عمل الأجهزة الحاسوبية أو المعلومات المخزنة بها في الحالات التي لم يفرض قانون مكافحة الجريمة المعلوماتية عقاب عليها.

---

(1) مشار إلى هذه القضية عند د.جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، المرجع السابق، ص41.

(2) Eoghan Casey, op-cit, chapter 1, p-4.

الأعمال الدعائية والتحريض على ارتكاب الجرائم

نصت المادة 29 من قانون مكافحة الجريمة المعلوماتية على ما يلي:

(أ- يُعاقَب بالحبس من ستة أشهر إلى ثلاث سنوات والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية، كل من قام بالتحريض أو بالترويج لارتكاب أي جريمة من الجرائم المنصوص عليها في القوانين الجزائية النافذة باستخدام الشبكة.

ب- ولا تقلّ عقوبة الحبس عن سنة والغرامة عن مئتين وخمسين ألف ليرة سورية، إذا ارتكِب الفعل المنصوص عليه في الفقرة (أ) من هذه المادة باستخدام الإنترنت).

ويقصد بالتحريض وفق المادة 216 من قانون العقوبات، حمل أو محاولة حمل شخص بأية وسيلة كانت على ارتكاب جريمة. والواقع أن مفهوم التحريض وأحكامه المنصوص عليها في القواعد العامة لا يختلف عن مفهومه المراد به في هذه المادة، فمن يقوم بتحريض شخص آخر على القتل عبر شبكة الانترنت، يمكن ملاحقته وفق القواعد العامة بجناية التحريض على القتل، كما يمكن ملاحقته وفق نص المادة 29 من قانون مكافحة الجريمة المعلوماتية بجنحة التحريض عبر الانترنت على ارتكاب هذه الجريمة، ففي هذا المثال نكون أمام حالة اجتماع جرائم معنوي وفق المادة 180 من قانون العقوبات، والتي توجب على القاضي ذكر جميع الأوصاف في حكمه، ثم أن يحكم بالعقوبة الأشد، وهي هنا جناية التحريض على القتل وفق القواعد العامة.

أما **الترويج** فيُقصد به، أعمال الدعاية على ارتكاب الجرائم التقليدية أو التعريف بطرق ارتكابها، فهو لا يرقى إلى مستوى التحريض، ومن الأمثلة على ذلك، إنشاء موقع إلكتروني على الانترنت للترويج لجريمة الاتجار بالأشخاص، يُنشر من خلاله آلية ارتكاب هذه الجريمة وحجم عائداتها المالية، أو إنشاء موقع إلكتروني للترويج لجريمة غسيل الأموال، أو جريمة الاحتيال أو السرقة من أماكن سكن الناس، وغير ذلك من الجرائم، ففي جميع هذه الحالات يسأل الفاعل عن جريمة الترويج وفق المادة 29 من قانون مكافحة الجريمة المعلوماتية مع تشديد المذكور في الفقرة ب لارتكاب الفعل باستخدام الانترنت.

وفي قضية حديثة عرضت على القضاء تتلخص بقيام شخص بإنشاء حساب باسم مستعار على أحد مواقع التواصل الاجتماعي، ثم قيامه بكتابة مقالات تتضمن إثارة النعرات الطائفية، بالإضافة إلى إرساله رسائل إلى عدة أشخاص تتضمن التحريض على التظاهر وارتكاب أعمال الشغب، وتحديد الزمان والمكان الذي يجب أن يتم التجمع به لارتكاب هذه الأعمال. وقد حُركت الدعوة العامة بحق الفاعل بجرم التظاهر والتحريض عليه عبر الانترنت،

وإثارة النعرات الطائفية عبر الانترنت[3].

وبعد أن انتهينا من دراسة الأحكام الموضوعية لجرائم المعلوماتية من خلال الفصل الأول، سننتقل إلى دراسة الأحكام الإجرائية لهذه الجرائم في الفصل الثاني.

([3]) سجلات النيابة العامة بدمشق القضية رقم موجوداً 5866/م تاريخ 2012/6/2، وهي منظورة أمام محكمة بداية الجزاء الخامسة بدمشق برقم أساس 1215 لعام 2012.

تمارين:

اختر الإجابة الصحيحة: في الجرائم التقليدية التي ترتكب على شبكة الإنترنت:

1. يجب أن يكون للشبكة دور ثانوي في ارتكاب الجريمة.
2. يجب أن يكون للشبكة دور ايجابي في ارتكاب الجريمة.
3. يجب أن يرتكب النشاط الجرمي عبر الشبكة.
4. الاجابتان الثانية والثالثة صحيحتان.

الإجابة الصحيحة رقم 4

الأحكام الإجرائية للجريمة المعلوماتية

الوحدة التعليمية الرابعة

1- الإختصاص القضائي

الكلمات المفتاحية:

الموقف القانوني والقضائي المقارن من مسألة الاختصاص- مسألة الاختصاص في ظل التشريع السوري- الصلاحية.

الملخص:

هنالك العديد من الحلول المتبعة في حل مشكلة الاختصاص القضائي فيما يتعلق بجرائم المعلوماتية وخاصة جرائم الإنترنت، إضافة إلى أن المشرع المقارن له موقف خاص في مشاكل الإحتصاص إضافة الى المشرع السوري.

الأهداف التعليمية:

في نهاية هذه الوحدة التعليمية يجب أن يكون الطالب قادراً على:

1- تمييز كيفية تطبيق الصلاحية الاقليمية والذاتية والشخصية والعالمية على جرائم المعلوماتية وخاصة جرائم الإنترنت

2- شرح مبررات اعتبار النطاق العلوي السوري أنه جزء من الاقليم السوري.

إن الجوانب الإجرائية لجرائم المعلوماتية هي التي تنقل نص التجريم من حالة الركود إلى حالة الحركة. فنجاح القواعد الموضوعية سيبقى مرهوناً بمدى إمكانية تطبيق هذه النصوص على أرض الواقع، مع مراعاة ما يحتاجه هذا التطبيق من إمكانيات تقنية تختلف بحسب مستوى التقدم التقني والتكنولوجي في كل دولة.

فعند الانتقال إلى دائرة التطبيق العملي لجرائم المعلوماتية، تظهر التحديات التي تبدأ من مسألة الاختصاص القضائي، مروراً بأعمال الاستدلال والتحقيق، وانتهاءً بقضية الإثبات؛ حيث اعتادت الضابطة العدلية أن تكون أدلة الإثبات مادية ملموسة، وهذا ما لا يتحقق دوماً في جرائم المعلوماتية.

الاختصاص القضائي

إن طبيعة الجغرافيا على الإنترنت، والإمكانيات التقنية العالية التي تتيحها هذه الشبكة، يمكن أن يؤدي إلى اقتراف النشاط الجرمي في دولة، وتحقق النتيجة الجرمية في دولة أخرى. الأمر الذي يثير مشكلة تنازع القوانين الجزائية من حيث المكان، أو ما يعرف بالاختصاص الجزائي الدولي.

و يقصد بالاختصاص "السلطة التي يقررها المشرع للقضاء لأن ينظر في دعاوى معينة حددها القانون"[1]، فالاختصاص في المسائل الجزائية هو ولاية القاضي في نظر دعوى جزائية معينة[2].

والاختصاص على نوعين: دولي وداخلي، ويقصد بالاختصاص الدولي، الحالات التي يكون فيها القانون الجزائي في دولة ما مختصاً بنظر دعاوى معينة، أما الاختصاص الداخلي فيقصد به، توزيع الدعاوى الجزائية وفق معايير محددة داخل الدولة، بعد أن ينعقد لها الاختصاص الدولي، فبحث الاختصاص الدولي يسبق البحث في الاختصاص الداخلي.

وإذا كانت قواعد تنازع القوانين من حيث المكان في القانون المدني، تقرر مبدأً أساسياً هو عدم التلازم بين الاختصاص القضائي والاختصاص التشريعي، فإن الأمر في إطار القانون الجزائي على العكس تماماً، إذ إن هناك تلازماً بين نطاق تطبيق القانون الجزائي واختصاص المحاكم الجزائية. وهذا ما هو مطبق في تشريعنا السوري؛ فكل جريمة يسري عليها قانون العقوبات السوري تختص بها حكماً المحاكم الجزائية السورية دون غيرها.

ومسألة الاختصاص القضائي في جرائم الحاسوب لا تثير أية مشكلة إذا ما ارتكبت الجريمة داخل إقليم الدولة. أما الاختصاص القضائي عبر العالم الافتراضي أو الإنترنت فيعد من المشكلات المعاصرة التي واجهت الفقه الإجرائي؛ إذ إن المشكلة الأساسية لجرائم الإنترنت تكمن في أنها لا تعرف حدوداً جغرافية، ناهيك عن أن الإنترنت ليست ملكاً لأحد، ولا تخضع لسيطرة دولة معينة. لذلك تتعدد القوانين الجزائية التي يمكن أن تحكم جرائم هذه الشبكة بتعدد الدول المرتبطة بها.

والاتجاه الغالب في العالم اليوم، لحل مشكلة الاختصاص القضائي عبر الإنترنت، هو تطبيق المبادئ ذاتها المعمول بها لحل مشكلة الاختصاص الجزائي الدولي في الجرائم التقليدية، وعلى رأسها **مبدأ إقليمية القانون الجزائي**، أي تطبيق القانون الجزائي على جميع الجرائم التي ترتكب في إقليم الدولة أيّاً كانت جنسية مرتكب الجريمة. كما استعان هذا الاتجاه في كثير من الأحيان بالمبادئ الأخرى التي تؤدي إلى امتداد القانون الجزائي خارج إقليم الدولة وتوسيع مساحة الاختصاص. وهذه المبادئ هي:

---

(1) د.محمود نجيب حسني: شرح قانون الإجراءات الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة، عام 1988، ص359.

(2) د. حسن الجوخدار: أصول المحاكمات الجزائية، من ثلاثة أجزاء، الطبعة الخامسة، منشورات جامعة دمشق، عام 1991، الجزء الثاني، ص81.

- **مبدأ عينية النص الجزائي أو الصلاحية الذاتية**، أي تطبيق النص الجزائي على الجرائم التي تمس المصالح الأساسية للدولة، ولو ارتكبت الجريمة خارج إقليم الدولة، وأيّاً كانت جنسية مرتكبها.
- **مبدأ شخصية النص الجزائي**، أي تطبيق النص الجزائي على كل جريمة يرتكبها من يحمل جنسية الدولة، ولو ارتكبت الجريمة خارج إقليمها.
- **مبدأ عالمية النص الجزائي أو الصلاحية الشاملة**، أي تطبيق النص الجزائي على كل جريمة مرتكبة خارج إقليم الدولة، إذا كان الجاني أجنبياً ومقيماً على إقليمها، ولم يكن قد طُلب تسليمه إلى إحدى الدول لمحاكمته أو قُبل.

الموقف القانوني والقضائي المقارن من مسألة الاختصاص

تعددت الطرائق والهدف واحد. فعلى الرغم من لجوء معظم الدول إلى مبدأ إقليمية النص الجزائي والمبادئ الأخرى المشار إليها لحل مشكلة الاختصاص القضائي على الإنترنت، إلا أن طريقة تبنّي هذا الحل اختلفت من دولة إلى أخرى. فبعض الدول تبّنت هذا الحل عن طريق الاتفاقيات الدولية، أو من خلال تشريعاتها الداخلية. وبعضها الآخر توسع قضاؤها في تفسير هذه المبادئ ليطبقها على جرائم الإنترنت. لذلك لا بد لنا من دراسة أبرز الاتفاقيات والتشريعات التي تعرضت لمسألة الاختصاص، إضافةً إلى الموقف القضائي والفقهي في هذا المجال.

أولاً- الاتفاقية الأوربية حول الجريمة الافتراضية لعام 2001:

أشارت المادة /22/ من هذه الاتفاقية إلى المبادئ التي يجب على الدول الأطراف اعتمادها، لتحديد الاختصاص القضائي فيما يتعلق بالجرائم المنصوص عليها في هذه الاتفاقية، وهذه المبادئ هي:

أ-مبدأ الإقليمية:

نصت على هذا المبدأ الفقرة (1) البند (a) من المادة /22/، وقد طلب هذا البند من كل دولة طرف في هذه الاتفاقية أن تعاقب على الجرائم المنصوص عليها، إذا ارتكبت الجريمة ضمن النطاق الإقليمي للدولة.

وعلى سبيل المثال يعد هذا الاختصاص منعقداً، إذا كان نظام الحاسوب العائد للمعتدي ضمن الإطار الإقليمي، ولو كان المعتدي مقيماً خارج الدولة، أو إذا كان نظام الحاسوب العائد للضحية ضمن الإطار الإقليمي للدولة.

كما يعدّ الاختصاص الإقليمي متوفراً وفق هذا البند، إذا كان مصدر الإرسال أو جهة الوصول داخل إقليم الدولة.[3]

ب-مبدأ نسبية الاختصاص المكاني (الإقليم الاعتباري):

نصت على هذا المبدأ الفقرة (1) البندين (c و b) من المادة /22/، وقد طلب هذان البندان من كل دولة طرف بالاتفاقية أن تكون مختصة جزائياً بالجرائم المرتكبة على السفن التي ترفع علم الدولة أو الطائرات المسجلة وفقاً للقانون فيها[4].

---

(3) د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية،الطبعة الثانية، مؤسسة آدم للنسر والتوزيع، مالطا، ص181.

(4) د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية، المرجع السابق، ص182.

ج- مبدأ الجنسية:

نصت على هذا المبدأ الفقرة (1) البند(D) من المادة /22/، وقد طلب هذا البند من الدول الأطراف أن تكون مختصة جزائياً عندما يرتكب مواطنو أي من هذه الدول جريمة في الخارج، إذا كان هذا السلوك يشكّل جريمة وفق قانون الدولة التي ارتكبت على أرضها الجريمة[5].

د- مبدأ التعاون الدولي في مكافحة الإجرام أو الصلاحية الشاملة أو العالمية:

نصت على هذا المبدأ الفقرة (3) من المادة /22/، والتي تقضي بأنه في حال رفض أي دولة طرف في هذه الاتفاقية تسليم مرتكب الجريمة المتواجد على أرضها، على أساس مبدأ الجنسية، فيجب على الدولة الرافضة القيام بإجراءات التحقيق والمحاكمة، وفقاً لقانونها الوطني.

ولقد سمحت الفقرة (2) من المادة /22/ من هذه الاتفاقية للدول الأطراف بالتحفظ على هذه المعايير، ولكن لا يجوز التحفظ في نقطتين: الأولى مبدأ الإقليمية، والثانية عندما يكون هناك على الدولة التزام بالتسليم[6].

كما سمحت الفقرة (4) من المادة /22/، للدول الأطراف أن تتخذ أشكالاً أخرى من معايير الاختصاص على نحو يتناسب مع قانونها الوطني.

وإذا كانت جريمة الحاسوب تدخل في اختصاص أكثر من دولة من الدول الأطراف (مثل جرائم العدوان الفيروسي أو الاحتيال وغيرها)، فإن على هذه الدول التشاور فيما بينها لتحديد المكان الملائم للمحاكمة، حتى يتم تجنب ازدواج الجهود المبذولة، والإزعاج غير الضروري للشهود، أو المنافسة بين السلطات الرسمية في الدول ذات العلاقة (الفقرة /5/ من المادة /22/)[7].

أما التعاون الدولي بين أطراف هذه الاتفاقية، فقد جاءت أحكامه في الفصل الثالث منها.

ثانياً- القانون العربي الاسترشادي (النموذجي) لمكافحة جرائم تقنية أنظمة المعلومات وما في حكمها لعام 2004:

نصت المادة /26/ من هذا القانون (النموذجي)، تحت عنوان "**إطار تطبيق القانون**" على ما يلي: (تسري أحكام هذا القانون على أي من الجرائم المنصوص عليها فيه، حتى ولو ارتكبت كلياً أو جزئياً

---

(5) د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية، المرجع السابق، ص183.

(6) د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية، المرجع السابق، ص184.

(7) د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية، المرجع السابق، ص185.

خارج إقليم الدولة، متى أضرّت بأحد مصالحها، ويختص القضاء الوطني بنظر الدعاوى المترتبة عليها)[8].

ومن الملاحظ أن هذا القانون (النموذجي) عالج مسألة الاختصاص في جرائم الإنترنت على استحياء، إذ إن هذا النص الوحيد لم يأخذ بعين الاعتبار الجرائم التي تدخل ضمن نطاق مبدأ الجنسية ومبدأ العالمية.

ثالثاً– الولايات المتحدة الأمريكية:

لجاء القضاء الأمريكي لحل مشكلة الاختصاص إلى مبدأ الاختصاص الشخصي "PERSONAL JURISDICTION " المقرر في الدستور الأمريكي، والذي يجعل المحاكم الأمريكية تختص بنظر جرائم الإنترنت في حالتين، هما:

الأولى: وجود مرتكب الجريمة في الدولة.

الثانية: أن يكون لمرتكب الجريمة وجوداً كافياً في الدولة، أي أن يكون للجاني حد أدنى من الاتصال بالولايات المتحدة الأمريكية[9].

وقد طبق القضاء الأمريكي مبدأ الاختصاص الشخصي بطرق متعددة. ويمكن تلخيص هذه الطرق ضمن ثلاث نظريات، هي:

أ–نظرية الإطلاق أو امتداد النتيجة:

في عام 1997، أصدر النائب العام في ولاية "مينيسوتا" الأمريكية إعلاناً، يتضمن تحذيراً إلى مستخدمي ومزودي خدمة الإنترنت، حيث اعتبر الإعلان أن كل جريمة من جرائم الإنترنت، يمكن أن يصل بثها إلى ولاية "مينيسوتا" تكون قوانين الولاية مختصة بها، حتى ولو ارتكبت الجريمة خارج حدود الولاية، بحيث يبدو الأمر كما لو قام الجاني بإطلاق الرصاص من خارج حدود الولاية على شخص داخل الولاية، فتكون قوانين الولاية مختصة في هذه الحالة. وقد طبق قضاء ولاية "مينيسوتا" هذا المبدأ بشأن جريمة بث موقع لألعاب القمار عبر الإنترنت من "لاس فيغاس" بولاية "نيفادا"، والذي وصل بثه بطبيعة الحال إلى ولاية "مينيسوتا"[10].

---

(8) د.عبد الله عبد الكريم عبد الله: جرائم المعلوماتية والإنترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت،2001، ص147.

(9) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص90.

(10) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص 886 و 909.

ب – نظرية الحد الأدنى للاتصال:

لخّصت المحكمة الاتحادية العليا في أمريكا المبادئ الأساسية للاختصاص القضائي، بأن من حق المحكمة ممارسة اختصاص قضائي شخصي على المتهم غير المقيم في الولاية، إذا كان هذا المتهم له صلات دنيا بالمجتمع، أو إذا كانت إقامة الدعوى عليه لا تؤذي فكرة المحاكمة العادلة(11).

ويعود التطبيق الأول للاختصاص القضائي على الإنترنت المتعلق بفكرة الحد الأدنى للاتصال إلى عام 1996، وذلك في قضية نُظرت في شمال أمريكا، وتتلخص وقائع هذه القضية بما يلي:

أن شركة INSET SYSTEM المحدودة، وهي شركة مقرها في ولاية "كونيكيتكوت" Connecticut قامت برفع قضية سرقة علامة تجارية ضد شركة INSTRUCTION SET التي مقرها في ولاية "ماساشوسيتش" Massachusetts، لأن هذه الأخيرة قامت بتقليد الموقع الإلكتروني للشركة الأولى وهو (Inset.com)، حيث كانت الشركة المنتهكة لهذه العلامة تقوم عبر هذا الموقع بعرض بضائعها وخدماتها عبر الإنترنت، الأمر الذي أثار حفيظة الشركة المالكة لهذه العلامة التجارية.

وقد تم رفع القضية في ولاية "كونيكتيكوت"، حيث طرحت المحكمة على نفسها السؤال التالي:

هل يتوفر في هذه القضية الحد الأدنى للاتصال وفق معيار المحكمة الاتحادية العليا؟

وقد قبلت المحكمة هذه القضية، وبررت قرارها بأن الشركة المعتدية وجّهت نشاطها الإعلاني بشكل مقصود إلى ولاية "كونكيتكوت"، لذلك من المنطقي أن يتم الادعاء عليها هناك(12).

كما استخدم القضاء الأمريكي في مسألة الاختصاص القضائي عبر الإنترنت معيار المواقع الإيجابية والمواقع السلبية، أو ما يُعرف **باختبار السلبية.** ويقصد **بالمواقع الإلكترونية السلبية** المواقع التي تقدم المعلومات فقط، أما **المواقع الإلكترونية الإيجابية** فهي التي تقوم بالتفاعل مع زبائنها، حيث يعتبر الاختصاص القضائي منعقداً إذا كان الموقع إيجابياً(13).

وتطبيقاً لذلك، فقد قامت شركة "بنسوسان" للمطاعم Bensusan Restaurant Corporation والتي تملك نادي ليلي باسم Blue Note مقره في "نيويورك"، وتملك علامته التجارية، برفع دعوى انتهاك لهذه العلامة ضد شخص يدعى "ريتشارد كينغ" Richard King، لأن هذا الأخير كان يدير نادياً ليلياً في "ميسوري" ويحمل ذات الاسم Blue Note. وقد أنشأ المدير المذكور موقعاً إلكترونياً بهذا الاسم، لتقديم معلومات عن النادي وعن مواعيد الحفلات.

---

(11) Adam D Thierer, Clyed wayne crews, Who rules the net?, published by cat to institute, 2003, P- 92 .

(12) Adam D Thierer, op-cit, P-94.

(13) Adam D Thierer, op-cit, P-93.

وقد أُقيمت الدعوى أمام محكمة نيويورك الفيدرالية، حيث قررت المحكمة بأنها غير مختصة بنظر الدعوى في ولاية نيويورك، وعلّلت قرارها بأن الموقع الإلكتروني للنادي الذي يديره السيد "كينغ" هو موقع سلبي غير فعّال، لأن من يريد شراء التذاكر، كان عليه السفر إلى "ميسوري"، لأن مكتب النادي لا يقوم بإرسال التذاكر بالبريد[14].

ج-نظرية الاستهداف:

اعتمدت معظم المحاكم في الولايات المتحدة الأمريكية مبدأ الاستهداف في الاختصاص القضائي على الإنترنت، والذي يتطلب أن يستهدف الموقع الإلكتروني سكان ولاية ما.

ففي عام 2001، رفعت شركة American Information Corp دعوى انتهاك علامة تجارية ضد شركة American Information المحدودة، وذلك أمام محكمة ولاية "ميرلاند"، التي قررت أنها غير مختصة قضائياً بنظر هذه الدعوى، لأن نشاطات البيع لم تستهدف سكان الولاية عبر موقعها الإلكتروني[15].

ومن الجدير بالذكر أن نقابة المحامين الأمريكية (ABA)[16]، قامت بإصدار دراسة عالمية حول الاختصاص القضائي للإنترنت، واقترحت بهذه الدراسة اعتماد مبدأ الاستهداف لحل مشكلة الاختصاص القضائي على الإنترنت[17].

رابعاً- بريطانيا:

بموجب قانون إساءة استعمال الكمبيوتر لعام 1990، فإن القضاء البريطاني يختص بالجرائم التي ينص عليها هذا القانون إذا اقترفت ضمن الاختصاص الإقليمي، أي إذا كان حاسوب الجاني أو حاسوب الضحية داخل إقليم الدولة[18]، كما تم إحداث اختصاصات قضائية حديثة بموجب قانون العدالة الجزائية البريطاني لعام 1993[19]، حيث تناولت هذه الاختصاصات معظم جرائم الاحتيال العابرة للحدود، وجرائم الابتزاز وغيرها[20].

---

(14) Adam D Thierer, op-cit, P-95.

(15) Adam D Thierer, op-cit, P-106.

(16) وهو اختصار لـ American Bar Association

(17) Adam D Thierer, op-cit, P-107.

(18) القاضي د. غسان رباح: المرجع السابق، ص167. د.عمر بن يونس، الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص911.

(19) Criminal Justice Act 1993 متوفر على الإنترنت على الموقع www.britishlaw.org.uk

(20) Micheal Hirst, Jurisdiction and the Ambit of the criminal law, published by oxford university, 2003, P-111-113.

وفي إحدى القضايا المعروضة على القضاء البريطاني، تمّت إدانة مواطن فرنسي مقيم في لندن، بجرم نشر المواد الفاحشة، حيث كان هذا الفرنسي يدير موقعاً على الإنترنت مخصصاً للمثليين جنسياً. وقد دفعت جهة الدفاع بعدم اختصاص القضاء البريطاني، لأن هذا الموقع كان مستضافاً على مُخدّم في الولايات المتحدة الأمريكية، إلاّ أن المحكمة الملكية أعلنت اختصاصها وأدانت المتهم، لأن هذه المواد الفاحشة تمّ نشرها في إنكلترا، كونها ظهرت على شاشة الحاسوب العائد لأحد الضباط المختصين في مكافحة هذه الجرائم في إنكلترا، ومن ثم فإن وصول البث إلى إنكلترا، يعدّ بمثابة ارتكاب الجريمة فيها[21].

<u>خامساً– فرنسا:</u>

تضمن قانون العقوبات الفرنسي لعام 1992 القواعد المتعلقة بتنازع القوانين الجزائية من حيث المكان، والمنصوص عليها في المواد (1– 113وحتى 7–113) منه[22].

وقد تضمنت هذه القواعد مبادئ الإقليمية والعينية والشخصية، التي قام القضاء الفرنسي بتطبيقها على جرائم الإنترنت. ففي إحدى القضايا التي عرضت على القضاء الفرنسي، تمّ إدانة مديري شركة "فرانس نت" France net و "ورد نت" World Net، لأنهما قاما بنشر صور دعارة أطفال آتية من الخارج[23]. وفي رأي الفقه، فإن وجود المخدم المضيف[24] في الخارج لا يؤثر على وقوع الجريمة، كما يعد فعل البث أحد العناصر المكونة للجريمة[25].

<u>سادساً– إيطاليا:</u>

طبق القضاء الإيطالي مبدأ الإقليمية المنصوص عليه بقانون العقوبات الإيطالي على جريمة القذف عبر الإنترنت، حيث اعتبرت محكمة النقض الإيطالية أن القذف عبر الإنترنت لا يختلف فحواه عن ذلك المقرر في قانون العقوبات الإيطالي، لأن كل صورة أو قول أو معلومة يتم بثها عبر الإنترنت، ويمكن رؤيتها من قبل مجموعة غير محدودة من الناس في أي مكان حول الكرة الأرضية، فهناك جريمة

---

(21) Michael Hirst, op-cit, P-188.

(2) قانون العقوبات الفرنسي متوفر على موقع القوانين الفرنسية www.legifrance,gouv.fr

(23) القضية متوفرة على www.francenet.fr مشار إليها عند : د.جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 2002، ص 50.

(24) **المضيف** Host, هو حاسوب يتصل به عدد من الطرفيات والحواسيب الأخرى، ويقوم بعمليات المحاسبة والمعالجة، ويمكّن الحواسيب الأخرى من الوصول إلى الملفات المخزنة فيه. وعند فتح حساب انترنت لدى المضيف، يقوم بحجز مساحة من الذاكرة لخدمة هذا الحساب، ويؤمن له الوسائل البرمجية اللازمة للتعامل وإدارة الاتصال. د.عبد الحسن الحسيني: المرجع السابق، ص406.

(25) د.جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، المرجع السابق، ص46 وما بعدها. د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص912.

تامة، ليس اعتباراً من الوقت الذي تمّ فيه بث الرسالة المجرّمة، وإنما من الوقت الذي أمكن فيه قراءة الرسالة من قبل الغير، وهذا ما يعرف **مبدأ الوجود في كل مكان،** إذ إن الجريمة تعد كما لو كانت قد وقعت في الأرض الإيطالية(26).

سابعاً- الإمارات العربية المتحدة:

طبق قضاء إمارة دبي مبدأ الإقليمية على واقعة قذف عبر الإنترنت، ارتكبتها إحدى الصحف الإلكترونية التي مقرها لندن، حيث كانت المجني عليها عند قراءة ألفاظ القدح موجودة في دبي. وقد اعتبرت المحكمة أنه طالما أن نتيجة الفعل تحققت في دبي، فإن الجريمة تعد قد وقعت في إقليم الدولة، وتخضع لأحكام قانون العقوبات الإماراتي(27).

ثامناً- مصر:

اجتهد الفقه المصري في حل مشكلة الاختصاص الجزائي عبر الإنترنت، حيث قام بتطبيق مبادئ الإقليمية والعينية والشخصية المقررة في قانون العقوبات المصري على جرائم الإنترنت؛ حيث اعتبر أن بثّ صور إباحية أو رسالة مُجرمة عبر الإنترنت، يعقد الاختصاص لقانون العقوبات المصري بمجرد وصول البث إلى مصر، ولو كان الفعل غير معاقب عليه في البلد الذي تمّ منه البث، ومن ثم فإن وجود المخدّم المضيف خارج إقليم الدولة لا أثر له على وقوع الجريمة(28).

وبعد هذه الجولة على الموقف القانوني والقضائي المقارن في مسألة الاختصاص، نجد أن معظم الدول قامت بتطبيق مبدأ الإقليمية والمبادئ الأخرى المعمول بها في تحديد الاختصاص الجزائي الدولي على جرائم الإنترنت، حيث اعتبرت وصول البث إلى إقليم الدولة هو أحد العناصر المكونة للجريمة، ولو كان المخدّم المضيف خارج إقليم الدولة.

---

(26) حكم محكمة النقض الايطالية متوفر على www.penale.it مشار إليه عند: د. عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، المرجع السابق، ص903.

(27) استئناف دبي (1248، 2003/1252) مشار إليه عند محمد الكعبي، المرجع السابق، ص62.

(28) د. جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، المرجع السابق، ص47 وما بعدها. د.أحمد حسام طه تمام: المرجع السابق، ص145 وما بعدها. فهد سلطان محمد أحمد بن سليمان: مواجهة جرائم الإنترنت (دراسة مقارنة)، رسالة ماجستير مقدمة إلى كلية الحقوق، جامعة القاهرة، 2004، ص111.

مسألة الاختصاص في ظل التشريع السوري

نصت المادة 33 من قانون مكافحة الجريمة المعلوماتية على ما يلي:

(أ–يُطبَّق على الجرائم المنصوص عليها في هذا القانون الأحكام المتعلّقة بالصلاحيات الإقليمية والذاتية والشخصية والشاملة المنصوص عليها في قانون العقوبات.

ب–يُعدّ النطاق العُلوي السوري في حكم الأرض السورية في معرض تطبيق هذا القانون.)

استعمل المشرع السوري في قانون العقوبات تعبير (الصلاحية) للدلالة على(الاختصاص)، وأخذ بأربعة مبادئ لتحديد اختصاصه الجزائي الدولي، هي: الصلاحية الإقليمية، والصلاحية الذاتية (أو العينية)، والصلاحية الشخصية، والصلاحية الشاملة (أو العالمية).

ومن الملاحظ أن المشرع السوري قد أخذ بالصلاحية الإقليمية كمبدأ أساسي، أسوة بالتشريع المقارن، إلاّ أنه لم يقنع بإنفراده، لذلك جمع بين هذه الصلاحيات الأربعة حتى تكمل بعضها البعض، كي يطال الجرائم المرتكبة خارج إقليم الدولة التي يرى فيها مساساً بمصالحه واعتباراته.

وسنتناول كيفية تطبيق هذه الصلاحيات على جرائم الإنترنت فيما يلي :

<u>أولاً– الصلاحية الإقليمية:</u>

يقصد بمبدأ إقليمية القانون الجزائي، أن القانون الجزائي لدولة ما يطبق على كل جريمة ترتكب على إقليم هذه الدولة، سواء أكان الجاني يحمل جنسية هذه الدولة أم يحمل جنسية دولة أجنبية، وسواء أكان المجني عليه مواطناً أم أجنبياً[29].

ولمبدأ إقليمية القانون الجزائي نتيجتان: الأولى إيجابية، وهي أن يكون للقانون الجزائي تطبيق شامل على كافة الجرائم المرتكبة على إقليم الدولة، الأمر الذي يؤدي بالضرورة إلى عدم تطبيق القوانين الجزائية الأجنبية على هذه الجرائم. أما النتيجة الثانية فسلبية، وهي تقضي بعدم تطبيق القانون الجزائي على أية جريمة ترتكب خارج حدود الدولة[30].

وقد أخذ المشرع السوري بمبدأ الإقليمية في المادة /15/ من قانون العقوبات، حيث نصت هذه المادة على ما يلي:

(1–يطبق القانون السوري على جميع الجرائم المقترفة في الأرض السورية.

---

(29) د.محمود نجيب حسني: شرح قانون العقوبات اللبناني – القسم العام، المجلد الأول، الطبعة الثالثة (معدلة ومنقحة)، منشورات الحلبي الحقوقية، بيروت، عام 1988، ص180. د.عبد الوهاب حومد: المفصل في شرح قانون العقوبات – القسم العام، المطبعة الجديدة، دمشق، عام 1990، ص1080. د. عبود السراج، المرجع السابق، ص165.

(30) د.محمود نجيب حسني: شرح قانون العقوبات اللبناني – القسم العام، المرجع السابق، ص180.

2–تعد الجريمة مقترفة في الأرض السورية:

أ–إذا تمّ على هذه الأرض أحد العناصر التي تؤلف الجريمة، أو فعل من أفعال جريمة غير متجزئة، أو فعل اشتراك أصلي أو فرعي.

ب–إذا حصلت النتيجة في هذه الأرض، أو كان متوقعاً حصولها فيها.)

ومن الملاحظ أن المشرع السوري في الفقرة الثانية من هذه المادة أراد أن يوسع من صلاحيته الإقليمية لتشمل مختلف الجرائم التي تهدد الحقوق المحمية بموجب القانون السوري، وقد استخدم في هذا التوسع الركن المادي (سلوك ونتيجة وعلاقة سببية) كمعيار لتحديد ما إذا كانت الجريمة قد وقعت على الأرض السورية أم لا[31]، وهو مسلكٌ مرحبٌ به، لأن الفقه والقضاء لم يقبلا بالركن المعنوي بمفرده كمعيار لتحديد الاختصاص[32].

والواقع أن تطبيق مبدأ الإقليمية على جرائم الإنترنت لا يثير أية صعوبة إذا كانت جميع عناصر الجريمة قد وقعت على الأرض السورية، فإذا قام شخص موجود في سورية مثلاً باستخدام الإنترنت لاختراق المنظومة المعلوماتية لأحد المصارف العاملة في سورية، ثم قام بتحويل أرصدة بعض الحسابات إلى حسابه المصرفي، فإن جميع عناصر جريمة الاحتيال تكون قد وقعت على الأرض السورية.

لكن تطبيق مبدأ الإقليمية ليس دوماً بهذه السهولة، فالغالب أن جريمة الإنترنت عابرة للحدود، وبالتالي فإن عناصر الجريمة تتوزع على أقاليم عدة دول، وقد اعتبر المشرع جريمة الإنترنت مقترفة على الأرض السورية، وفق الفقرة الثانية من المادة /15/ من قانون العقوبات السوري، في الحالات التالية:

1– إذا تمّ على الأرض السورية أحد العناصر التي تؤلف جريمة الإنترنت. ومثال ذلك، قيام شخص موجود في سورية بإنشاء موقع للاحتيال عبر الإنترنت– سواء كان الموقع مستضافاً على مُخدّم سوري أم أجنبي– ثم وقع ضحية هذا الموقع شخص مقيم في الصين.

وغني عن البيان أن الأعمال التحضيرية لا تدخل ضمن عناصر الجريمة، ولا ترتقي إلى الأفعال التنفيذية، فلو قام شخص مقيم في لبنان مثلاً بإرسال رسالة إلكترونية إلى شخص مقيم في الصين، تتضمن فوز المرسل إليه بجائزة وهمية بقصد الاحتيال عليه، فإن القانون السوري لا يطبق لمجرد قيام الجاني بشراء الحاسوب من سورية.

(31) د. عبود السراج، المرجع السابق، ص166.

(32) د.عبد الوهاب حومد: المرجع السابق، ص1093.

2- إذا تمّ على الأرض السورية فعل من أفعال جريمة غير متجزئة. ويدخل في مفهوم الجريمة غير المتجزئة، الجريمة المستمرة والجريمة المتتابعة وجريمة العادة. فجريمة الاحتيال مثلاً من الممكن أن تكون متتابعة (متعاقبة)، فإذا قام شخص موجود في لبنان مثلاً، بالاحتيال على شخص موجود في سورية عن طريق البريد الإلكتروني، ثم قام هذا الجاني بالاحتيال عدة مرات على ذات المجني عليه، عن طريق الإنترنت، ففي هذه الحالة تكون جريمة الاحتيال متتابعة (متعاقبة) بسبب وحدة الإرادة الجرمية، ووحدة الحق المعتدي عليه، ووحدة الغرض.

3- إذا وقع على الأرض السورية فعل اشتراك أصلي أو فرعي. كما لو اشترك شخص موجود في سورية مع شخص آخر موجود في اليابان بعملية اختراق لمنظومة معلوماتية عبر الإنترنت عائدة لأحد المصارف الأمريكية بقصد الاحتيال فيتحقق هنا (الاشتراك الأصلي).

أما إذا قام شخص موجود في سورية بتقديم إرشادات لشخص موجود في اليابان، لاختراق منظومة معلوماتية عائدة لأحد المصارف الأمريكية بهدف تمكينه من الاحتيال. فيتحقق هنا التدخل (الاشتراك الفرعي).

4- إذا حصلت النتيجة الجرمية على الأرض السورية أو كان متوقعاً حصولها فيها. فإذا قام شخص موجود في كندا بإنشاء موقع للاحتيال عبر الإنترنت لتداول الأسهم الوهمية، ووقع ضحية هذا الموقع شخص موجود في سورية، فتكون النتيجة الجرمية هنا قد وقعت في سورية.

وتكون النتيجة متوقعاً حصولها في سورية وإن لم تحصل فعلاً. إذا قام شخص موجود في الإمارات مثلاً باستخدام بطاقة ائتمان مزورة للشراء من أحد المواقع الإلكترونية لشركة سورية، إلاّ أن الجريمة توقفت عند حد الشروع لظروف خارجة عن إرادة الفاعل.

وفي تقديرنا أن وصول البث إلى سورية لا يكفي بحد ذاته لانعقاد اختصاص القانون الجزائي السوري على أساس أن النتيجة وقعت في سورية، لأن مواقع الإنترنت يصل بثها بطبيعة الحال إلى أي مكان في العالم، بل لا بد من أن يكون المجني عليه موجوداً في سورية. وهذا التطبيق يشبه إلى حدٍ بعيد نظرية الاستهداف التي قام القضاء الأمريكي بتطبيقها.

وقد اعتبر المشرع السوري في الفقرة ب من المادة 33 من قانون الجريمة المعلوماتية أن النطاق العُلوي السوري في حكم الأرض السورية في معرض تطبيق هذا القانون. والنطاق العلوي السوري كما عرفته المادة الأولى من قانون مكافحة الجريمة المعلوماتية هو "اسم النطاق العُلوي الوطني للجمهورية العربية السورية؛ وهو ".سورية" و ".sy"، أو أي نطاق إضافي يُعتمد لاحقا".

و الواقع إن اعتبار تلك المساحة من الإنترنت، الخاضعة لإدارة الدولة السورية جزءاً من الإقليم الاعتباري السوري أو بحكم الأرض السورية، أمر يفرضه المنطق و الاعتبارات العملية، للسببين التاليين:

- إن المبررات المتعلقة بسيادة الدولة على إقليمها، والتي دفعت المشرع الجزائي إلى اعتبار الطائرة أو السفينة السورية بحكم الأرض السورية، متوفرة في ذلك **النطاق العلوي السوري** على الإنترنت، الذي يخضع لإدارة الحكومة السورية (المنتهي بـ sy) فهذا النطاق يحمل العلم السوري أو الجنسية السورية، وبالتالي فإن اعتباره بحكم الأرض السورية يتفق مع فلسفة المشرع السوري.

- هناك مبررات عملية تدفعنا إلى اعتبار النطاق الوطني السوري على الإنترنت بحكم الأرض السورية، وهي أن هناك جرائم من الممكن أن ترتكب عبر هذا النطاق السوري، دون أن تطولها قواعد الاختصاص الجزائي الدولي السورية، ونضرب على ذلك المثال التالي:

إذا أنشأت شركة فرنسية موقعاً إلكترونياً لها على النطاق السوري المنتهي بـ (SY.)، ثم قامت عبر هذا الموقع بالاحتيال على بعض الإيطاليين الموجودين في إيطاليا، فإن هذه الجريمة لا تخضع للقانون الجزائي السوري، لأن قواعد الاختصاص الدولي لا تسمح بذلك، فلا تنطبق على هذا المثال الصلاحية الإقليمية أو الشخصية أو الذاتية أو الشاملة، مع العلم أن الجريمة تمّت عبر النطاق الوطني السوري على الإنترنت.

ثانياً– الصلاحية الذاتية أو العينية:

يقصد بمبدأ الذاتية أو العينية، تطبيق القانون الجزائي على الجرائم التي تمسّ المصالح الأساسية للدولة، والمرتكبة خارج إقليمها، أيّاً كانت جنسية مرتكبها. وهذا المبدأ يفرضه حرص الدولة على حماية مصالحها الأساسية[33].

وقد أخذ المشرع السوري بهذا المبدأ في المادة /19/ من قانون العقوبات، التي نصت على ما يلي:

1ـ يطبق القانون السوري على كل سوري أو أجنبي، فاعلاً كان أو محرضاً أو متدخلاً، أقدم خارج الأرض السورية على ارتكاب جناية أو جنحة مخلّة بأمن الدولة، أو قلّد خاتم الدولة، أو قلّد أو زوّر أوراق العملة أو السندات المصرفية السورية أو الأجنبية المتداولة شرعاً أو عرفاً في سورية.

2–على أن هذه الأحكام لا تطبق على الأجنبي الذي لا يكون عمله مخالفاً لقواعد القانون الدولي.).

وتطبيقاً لذلك، فإن بعض الجرائم المحددة في هذا النص يمكن أن ترتكب عبر الإنترنت، فإذا قام شخص موجود في الخارج باختراق المنظومة المعلوماتية العائدة لوزارة الدفاع السورية عبر الإنترنت،

(33) د. عبود السراج: المرجع السابق، ص175. د.محمود نجيب حسني: شرح قانون العقوبات اللبناني – القسم العام، المرجع السابق، ص197. د.عبد الوهاب حومد: المرجع السابق: ص1095.

بقصد الحصول على معلومات سرية، يكون مرتكباً لجريمة التجسس المنصوص عليها بالمادة /272/ عقوبات. و أيضاً من يقوم في الخارج بنشر كتابات عبر الإنترنت لم تجزها الحكومة السورية، فعكّر صلات سورية بدولة أجنبية، يكون مرتكباً لجريمة ماسة بالقانون الدولي حسب المادة /278/ عقوبات.

ثالثاً– الصلاحية الشخصية:

يطبق مبدأ الصلاحية الشخصية بطريقتين: إيجابية وسلبية. ويقصد **بالطريقة الإيجابية** تطبيق القانون الجزائي على مرتكب الجريمة الذي يحمل جنسية الدولة ولو ارتكبت الجريمة خارج إقليمها. أما **الطريقة السلبية،** فيقصد بها تطبيق القانون الجزائي على كل جريمة يكون المجني عليه حاملاً لجنسية الدولة، ولو ارتكبت الجريمة خارج إقليمها، وأيّاً كانت جنسية مرتكب الجريمة.

وتطبيق مبدأ الشخصية بالطريقة الإيجابية، يؤدي إلى تجنب فرار المجرم الذي يسيء إلى سمعة وطنه عندما يرتكب جريمته خارج إقليم دولته ثم يفر إليها، إذ إن دولته لا تستطيع معاقبته على أساس مبدأ الإقليمية، ولا تستطيع تسليمه إلى الدولة التي ارتكب الجرم على أرضها، لأنه من رعاياها كما هو سائد في معظم التشريعات الجزائية. أما تطبيق مبدأ الشخصية بالطريقة السلبية، فهو يؤمن حماية رعايا الدولة من الاعتداءات الجرمية عليهم[34].

والمشرع السوري أخذ بمبدأ الشخصية في وجهه الإيجابي فقط بالمادة /20/ من قانون العقوبات، ولم يأخذ بهذا المبدأ في وجهه السلبي، لأنه انطلق من مبدأ الثقة بالقضاء الأجنبي، وقدرته على حماية المواطنين السوريين، إذا ارتكبت بحقهم جرائم معاقب عليها في القانون الأجنبي.

وقد نصت المادة /20/ من قانون العقوبات على ما يلي:

(يطبق القانون السوري على كل سوري، فاعلاً كان أو محرضاً أو متدخلاً، أقدم خارج الأرض السورية، على ارتكاب جناية أو جنحة يعاقب عليها القانون السوري.

و يبقى الأمر كذلك ولو فقد المدعى عليه الجنسية السورية أو اكتسبها بعد ارتكاب الجناية أو الجنحة.).

كما أكّد المشرع السوري بالمادة /21/ من قانون العقوبات، على تطبيق هذا المبدأ بالنسبة للجرائم التي يقترفها الموظفون السوريون في الخارج، أثناء ممارستهم وظائفهم أو بمناسبة ممارستهم لها، وعلى الجرائم التي يرتكبها أيضاً موظفو السلك الخارجي والقناصل السوريون الذين يتمتعون بالحصانة الدبلوماسية.

والمشرع السوري لم يأخذ بمبدأ الشخصية على إطلاقه في جميع الجنح التي يرتكبها المواطن

(34) د.محمود نجيب حسني: شرح قانون العقوبات اللبناني – القسم العام، المرجع السابق، ص 201– 202.

السوري في الخارج، فبحسب المادة 24 من قانون العقوبات يمكن أن نميز في نطاق الجنحة بين حالتين[35]:

1- إذا كانت الجنحة المرتكبة من قبل السوري في الخارج معاقباً عليها بالحبس ثلاث سنوات فأكثر وفق القانون السوري، فإن القانون السوري يطبق على الجاني دون النظر فيما إذا كان القانون الأجنبي يعاقب عليها أم لا.

2- إذا كانت الجنحة المرتكبة من قبل السوري في الخارج معاقباً عليها بالحبس أقل من ثلاث سنوات وفق القانون السوري، فيجب أن يكون القانون الأجنبي في هذه الحالة قد عاقب على هذه الجنحة أيضاً بعقوبة مهما كان نوعها، حتى نستطيع تطبيق القانون السوري، أي يجب أن يتحقق شرط المعاقبة في القانون الأجنبي، أما إذا لم يكن القانون الأجنبي قد نص على أية عقوبة لهذا الفعل، فإن القانون السوري لا يمكن تطبيقه.

أما في الجنايات، فمبدأ الشخصية يطبق على إطلاقه، فكل سوري ارتكب جناية في الخارج، سواء أكان القانون الأجنبي يعاقب عليها أم لا، يعاقب وفق القانون السوري .

وتطبيقاً لذلك، فالسوري الذي يقوم في الخارج بإنشاء موقع على الإنترنت ينتحل فيه الاسم التجاري لإحدى الشركات، ويقوم من خلاله بالاحتيال على شخص موجود خارج سورية أيضاً، يمكن ملاحقته وفقاً للصلاحية الشخصية، لأن عقوبة الاحتيال عبر الشبكة وفق المادة 21 من قانون مكافحة الجريمة المعلوماتية هي الحبس من ثلاث إلى خمس سنوات والغرامة من خمسمئة ألف إلى مليونين ونصف مليون ليرة سورية. أما في جرائم المعلوماتية الأخرى التي لا تصل فيها العقوبة إلى الحبس ثلاث سنوات، فيجب أن يتحقق شرط المعاقبة في القانون الأجنبي حتى نستطيع تطبيق مبدأ الصلاحية الشخصية.

<u>رابعاً- الصلاحية الشاملة:</u>

أخذ المشرع السوري بهذا المبدأ في المادة /23/ من قانون العقوبات، التي نصت على ما يلي:

(يطبق القانون السوري على كل أجنبي مقيم على الأرض السورية، أقدم في الخارج سواء أكان فاعلاً أو محرضاً أو متدخلاً، على ارتكاب جناية أو جنحة غير منصوص عليها في المواد 19، 20، 21 إذا لم يكن استرداده قد طلب أو قُبل.).

و لا يعد هذا الاختصاص، اختصاصاً رئيسياً وإنما هو اختصاص ثانوي أو احتياطي. أي أن

(35) د.عبد الوهاب حومد: المرجع السابق، ص1098. د. عبود السراج: المرجع السابق، ص 183. د.محمود نجيب حسني: شرح قانون العقوبات اللبناني – القسم العام، المرجع السابق، ص 213.

سورية لا تعاقب المجرمين الذين يقيمون على أرضها، إلاّ إذا لم يوجد من يعاقبهم من الدول الأجنبية.

وينطوي هذا الاختصاص على نوع من التعاون أو التضامن الدولي في مكافحة الإجرام، فهو يضمن عدم إفلات المجرمين الذين سولت لهم أنفسهم ارتكاب الجرائم في دولة، ثم الفرار إلى دولة أخرى تخلصاً من المسؤولية(36).

وعليه فالأجنبي الذي يرتكب جريمة في الخارج، ويلقى القبض عليه في سورية، يمكن محاكمته بموجب هذا الاختصاص الشامل، ولو لم يكن للقانون السوري اختصاص رئيسي في محاكمته، بشرط أن لا تطلب دولة أجنبية تسليمه من سورية، أو طلبت تسليمه لكن سورية رفضت التسليم، كأن يكون لاجئاً سياسياً مثلاً.

وتطبيقاً لذلك، فإذا قام هولندي موجود في الخارج مثلاً، باختراق منظومة معلوماتية عائدة لمصرف إيطالي، وقام بتحويل الأرصدة إلى حسابه احتيالاً، ثم جاء إلى سورية وألقي القبض عليه فيها، فيمكن محاكمته وفقاً للصلاحية الشاملة إذا لم يكن استرداده قد طلب من سورية أو قُبل.

---

(36) د. عبود السراج: المرجع السابق، ص 178- 179. د.عبد الوهاب حومد: المرجع السابق، ص1103-1104. د.محمود نجيب حسني: شرح قانون العقوبات اللبناني – القسم العام، المرجع السابق، ص 208-209.

تمارين:

اختر الإجابة الصحيحة: النطاق العلوي السوري:

1. لا يعتبر جزء من الاقليم السوري.
2. يدخل في الصلاحية العالمية فقط.
3. يدخل في الصلباحية الشخصية فقط.
4. يعتبر جزء من الاقليم السوري.

الإجابة الصحيحة رقم 4

الأحكام الإجرائية للجريمة المعلوماتية

الوحدة التعليمية الخامسة

2- الضابـطة العدليـة

الكلمات المفتاحية:

الأجهزة المختصة بمكافحة جرائم المعلوماتية-اختصاصات الضابطة العدلية في مكافحة جرائم المعلوماتية-تقديم الشكوى أو الاخبار- استقصاء الجرائم- القبض- التفتيش-الضبط.

الملخص:

تتضمن هذه الوحدة التعليمية التعرف على الأجهزة المختصة بمكافحة جرائم المعلوماتية على المستوى الاقليمي وعلى صعيد الدول وخاصة سورية، واختصاصات الضابطة العدلية في مكافحة جرائم المعلوماتية في الظروف العادية والإستثنائية.

الأهداف التعليمية:

في نهاية هذه الوحدة التعليمية يجب أن يكون الطالب قادراً على:

1- تمييز الأجهزة المختصة بمكافحة جرائم المعلوماتية على المستوى الاقليمي وعلى صعيد الدول وخاصة سورية

2- تمييز اختصاصات الضابطة العدلية السورية في مكافحة جرائم المعلوماتية في الظروف العادية والإستثنائية وهذه الاختصاصات هي: كيفية تقديم الشكوى أو الاخبار في جرائم المعلوماتية- استقصاء الجرائم- القبض- التفتيش-الضبط.

لا يبدأ تحريك الدعوى العامة من الفراغ، بل لا بد أن يبنى على أسباب معقولة أقلها اكتشاف الجريمة ومعرفة فاعلها وجمع أدلتها. فعند اكتمال هذه العناصر، تستطيع النيابة العامة ممارسة سلطتها التقديرية في إقامة الدعوى العامة أو عدم إقامتها. ومن هنا تظهر أهمية أعمال التحري أو الاستدلال، التي تبدأ منذ وقوع الجريمة وتستمر حتى تحريك الدعوى العامة. ويطلق الفقه في سورية على هذه المرحلة تسمية "مرحلة التحقيق الأولي أو التمهيدي"، أما الفقه في مصر وبعض البلدان الأخرى، فيطلق عليها "مرحلة جمع الاستدلالات"[1].

وفي جرائم المعلوماتية فإن أهمية هذه المرحلة تبلغ أعلى مستوياتها، لأنها تعد حجر الزاوية الذي سيتم على أساسه بناء الدعوى برمتها، فما يتم جمعه من معلومات وأدلة رقمية في المرحلة التي تعقب ارتكاب الجريمة مباشرة، قد لا يبقى متاحاً بعد مرور وقت قصير على ارتكابها، والسبب في ذلك يعود إلى الطبيعة التقنية لهذه الجرائم.

ففي كثير من جرائم المعلوماتية، لم يترك الجاني وراءه سوى ذلك التعبير الذي يعتري وجوه الذين قاموا بتعقبه، وهو تعبير ممزوج بالإحباط والإعجاب معاً، وتقليب الكفين على ما فات.

ولقد دفع تزايد هذه الجرائم المستحدثة معظم الدول إلى إنشاء أجهزة مختصة في مكافحتها على المستوى الوطني والإقليمي والدولي.

وفي سورية فإن الضابطة العدلية هي صاحبة الاختصاص العام في مكافحة جميع الجرائم، وجرائم المعلوماتية لا تخرج عن هذا الأصل العام. وللضابطة العدلية مجموعة من الاختصاصات، منها ما تمارسها في الظروف العادية، كاستقصاء الجرائم، وجمع الأدلة، وتلقي الإخبارات والشكاوى، وتنظيم المحاضر والضبوط. ومنها ما تمارسها في الظروف الاستثنائية، حيث تتسع صلاحيات هذه الضابطة، فتقوم بقسط وافر من وظائف قاضي التحقيق، كالقبض على فاعل الجريمة، والتفتيش، وضبط الأشياء الناتجة عن التفتيش.

([1]) د.حسن الجوخدار: المرجع السابق، الجزء الثاني، ص3.

الأجهزة المختصة بمكافحة جرائم المعلوماتية

أمام التزايد المستمر لجرائم المعلوماتية، لم تَسلم أجهزة الضبط القضائي من ضرورات التطور التقني والتكنولوجي. ونتيجةً لهذا التحدي قامت معظم الدول بإحداث أجهزة مختصة بمكافحة هذا النوع من الإجرام المستحدث، وقد حملت هذه الأجهزة تسميات مختلفة، منها شرطة الإنترنت، أو درك الإنترنت، أو متحري الإنترنت، وغير ذلك من التسميات.

وتختلف هذه الأجهزة عن الأجهزة المختصة بضبط الجرائم التقليدية من حيث طريقة التكوين، فهي لا تعتمد على التدريبات الجسدية التي يتلقاها عادةً رجال الشرطة، وإنما تعتمد على البناء العلمي والتكنولوجي لأفرادها، وهي تتولي مهمة التحري عن جرائم العالم الافتراضي لكشف النقاب عنها[2]. ولا يقتصر دور هذه الأجهزة على المستوى الوطني، بل هناك أجهزة مختصة على المستوى الدولي والأوربي. لذلك سوف نستعرض أهم هذه الأجهزة.

أولاً- الأجهزة المختصة بمكافحة جرائم المعلوماتية على المستوى الوطني:

ظهرت العديد من الأجهزة المختصة بمكافحة جرائم المعلوماتية على المستوى الوطني، سواء على صعيد الدول الأجنبية أم على صعيد الدول العربية. لذلك سنلقي الضوء على هذه الأجهزة الموجودة في هذه الدول.

أ-الدول الأجنبية:

كانت الدول المتقدمة سباقة بإحداث هذه الأجهزة؛ إذ إن مكافحة جرائم المعلوماتية يرتبط بمدى تقدم الدول من الناحية التقنية، وبمدى توفر الإمكانيات المادية اللازمة لإنشاء هذه الأجهزة.

1- الولايات المتحدة الأمريكية:

قامت الولايات المتحدة الأمريكية بإنشاء عدة أجهزة لمكافحة جرائم المعلوماتية، ومنها:

- شرطة الوبّ web police، وهي نقطة مراقبة على الإنترنت، إضافةً إلى أنها تقوم بتلقي الشكاوى من مستخدمي الشبكة، وملاحقة الجناة والقراصنة، والبحث عن الأدلة ضدهم وتقديمهم إلى المحاكمة[3].

---

(1) نبيلة هبه هروال: المرجع السابق، ص 99- 100.

(3) د.جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، المرجع السابق، ص 77.

• مركز تلقي شكاوى جرائم الإنترنت IC_3 [4]، الذي تمّ إنشاؤه من قبل مكتب التحقيقات الفيدرالي FBI في أيار عام 2000. وفي كانون الأول من عام 2003 تمّ دمج مركز شكاوى الاحتيال عبر الإنترنت المعروف بـ IFCC[5] مع هذا المركز. ويعمل مركز IC_3 بصورة تشاركية مع مكتب التحقيقات الفيدرالي، والمركز الوطني لجرائم الياقات البيضاء NW_3C[6].

ويقوم هذا المركز بتلقي الشكاوى عبر موقعه على الإنترنت، حيث يقوم الشاكي بملء استمارة إلكترونية، ثم يقوم المختصون في هذا المركز بتحليل الشكاوى وربطها بالشكاوى الأخرى المستلمة من قبل، ثم يتم إحالة المعلومات الناتجة عن عملية التحليل إلى الجهات المسؤولة عن تطبيق القوانين الأمريكية[7].

• قسم جرائم الحاسوب والعدوان على حقوق الملكية الفكرية الذي تمّ تأسيسه في عام 1991، ويختص هذا القسم بالتعريف بهذه الجرائم والكشف عنها وملاحقة مرتكبيها[8].

• نيابة جرائم الحاسوب والاتصالات CTC[9]، وتتألف من مجموعة من قضاة النيابة العامة الذين تلقوا تدريبات مكثفة على نظم المعالجة الآلية للبيانات، وتمّ منحهم صلاحيات واسعة في مجال الاستعانة بغيرهم من خبراء وزارة العدل، لا سيما قسم جرائم الحاسوب والعدوان على حقوق الملكية الفكرية، وهم مرتبطون بنظام تأهيلي وتدريبي مستمر [10].

• المركز الوطني لحماية البنية التحتية التابع للمباحث الفيدرالية الأمريكية. وقد حدّد هذا المركز البنى التحتية التي تعتبر هدفاً للهجومات والاعتداءات عبر الإنترنت، وعلى رأسها شبكات الاتصالات والمصارف وغيرها.

وإضافةً إلى هذه الأجهزة، يوجد أيضاً في الولايات المتحدة وحدة متخصصة بمكافحة الإجرام المعلوماتي تابعة لقسم العدالة الأمريكي، تتكون من خبراء في نظم الحوسبة والإنترنت، ومن مستشارين

(4) وهو اختصار لـ Internet Crime Complaint center، الموقع www.IC3.gov

(5) وهو اختصار لـ Internet Fraud Complaint center، الموقع www.ifcc.gov . Report of IC3 2004 Internet Fraud

(6) وهو اختصار لـ National white collar center، الموقع www.NW3C.org .

(7) Michael Kunz and Patrick Wilson, op-cit- 16.

(8) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق، ص 812.

(9) وهو اختصار لـ Computer and Telecommunication Coordinator

(10) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت,المرجع السابق، ص 893.

قانونيين[11].

2- بريطانيا:

قامت السلطات البريطانية بتخصيص وحدة تضم نخبة من رجال الشرطة المتخصصين في البحث والتنقيب عن جرائم الإنترنت، كالجرائم الجنسية الواقعة على الأحداث، والقرصنة ونشر الفيروسات وغيرها.

وتضم هذه الوحدة نحو /80/ عنصراً على درجة عالية من الكفاءة في المجال التقني. وقد بدأت هذه الوحدة نشاطها عام 2001 ومركزها لندن[12].

3- فرنسا:

قامت الحكومة الفرنسية بإنشاء عدة أجهزة لمكافحة جرائم المعلوماتية، نذكر منها:

- القسم الوطني لقمع جرائم المساس بالأموال والأشخاص، ويتكون هذا القسم من المحققين المختصين في التحقيق بجرائم العالم الافتراضي، وقد بدأ هذا القسم مهامه عام 1997.
- المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصالات. ويعد هذا المكتب سلاح الدولة الفرنسية في مكافحة جرائم الإنترنت، وقد تمّ إنشاؤه في 2000/5/15.
- تكوين مجموعة من الشرطة والدرك المتخصصين في التحقيق بجرائم الإنترنت[13].

4- اسبانيا:

قامت الحكومة الاسبانية بتأسيس وحدة التحريات المركزية المعنية بجرائم الإنترنت، وهي تعمل مع الإدارة المركزية في وزارة الداخلية على مراقبة مرتكبي هذه الجرائم وملاحقتهم[14].

5- بعض الدول الآسيوية:

* **هونكونغ:** قامت بتأسيس ما يعرف بـ "قوة مكافحة قرصنة الإنترنت" وذلك في كانون الأول عام 1999. وتمكّنت هذه القوة من إلقاء القبض على اثني عشر شخصاً في خمسة قضايا خلال مدة

---

(11) نبيلة هبه هروال: المرجع السابق، ص 108- 109.

(12) نبيلة هبه هروال: المرجع السابق، ص 111.

(13) نبيلة هبه هروال: المرجع السابق، ص 111 وما بعدها.

(14) نبيلة هبه هروال: المرجع السابق، ص 108.

ستة أشهر من إنشائها.

* **الصين:** قامت بتأسيس ما يعرف بـ "القوة المضادة للهكرة"، وهي تختص برقابة المعلومات التي يسمح لمواطنيها الدخول إليها عبر الإنترنت[15].

* **فيتنام:** قامت بتشكيل وحدة خاصة من الشرطة للتحقيق في جرائم الإنترنت، والحد من توزيع المنشورات المحظورة من خلالها[16].

ب-الدول العربية:

لم تقف الدول العربية مكتوفة الأيدي أمام الخطر المتزايد لجرائم المعلوماتية، فقد قامت بعض الدول بإنشاء أجهزة متخصصة لمكافحة هذه الجرائم. ومن بين هذه الدول:

1- مصر:

قامت جمهورية مصر العربية بتكليف بعض الجهات بمكافحة جرائم الإنترنت، ونذكر منها:

- الإدارة العامة لمباحث الأموال، وتختص هذه الإدارة بمكافحة الجرائم الاقتصادية، سواء كانت تقليدية أو مستحدثة كجرائم الإنترنت.

- الإدارة العامة للتوثيق والمعلومات، وتعتبر هذه الإدارة من أكبر الإدارات بوزارة الداخلية تعاملاً مع جرائم المعلوماتية. وفي عام 2002 تمّ إنشاء الإدارة العامة لمكافحة جرائم الحاسبات وشبكات المعلومات، وهي تابعة للإدارة العامة للتوثيق والمعلومات. وتتكون هذه الإدارة من ضباط على مستوى عالٍ من التخصص في مجال تكنولوجيا الحاسبات والشبكات، وتختص بمكافحة جرائم الإنترنت على مختلف أنواعها[17].

وإلى جانب هذه الأجهزة الحكومية، فقد تمّ تأسيس "الجمعية المصرية لمكافحة جرائم المعلوماتية والإنترنت"، وهي منظمة غير حكومية خاضعة للقانون المصري، ومشهرة تحت رقم /2176/ لعام 2005، وتهدف إلى تقديم الدعم العلمي للمؤسسات والأفراد، وتنمية الكوادر البشرية في مجال مكافحة

---

(15) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق، ص 812.

(16) نبيلة هبه هروال: المرجع السابق، ص 108.

(17) نبيلة هبه هروال: المرجع السابق، ص 141 ومابعدها.

الإجرام عبر الإنترنت[18].

2- الأردن:

في عام 1988، أنشأت الأردن قسماً خاصاً بجرائم الحاسوب تابعاً لمديرية الأمن، ويتعامل هذا القسم مع مختلف جرائم الحاسوب والإنترنت منذ ذلك العام[19].

وفي عام 2006، تمّ تأسيس جمعية خاصة باسم "الجمعية الأردنية للحد من جرائم المعلوماتية والإنترنت"، مركزها عمان، وتهدف إلى تقديم الدعم العلمي للمؤسسات والأفراد، وتنمية الكوادر البشرية في مجال مكافحة الإجرام عبر الإنترنت[20].

3- الجزائر:

قامت الجزائر بإنشاء مركز لمكافحة جرائم الإنترنت على مستوى الدرك الوطني، وقد بدأ مهامه في أواخر عام 2006 [21].

4-الإمارات العربية المتحدة:

قامت دولة الإمارات بتأسيس مركز الاستجابة لطوارئ الحاسب الآلي aeCERT[22] بقرار المجلس الوزاري للخدمات رقم (89/5) لسنة 2008، كفريق وطني للاستجابة لطوارئ الحاسب الآلي.

وهو مركز جديد من نوعه في الدولة، حيث قامت هيئة تنظيم الاتصالات بإنشائه لتحسين معايير وممارسات أمن المعلومات وحماية البنية التحتية لتقنية المعلومات بدولة الإمارات من مخاطر واختراقات الإنترنت. ومهمة هذا المركز هي دعم البنية التحتية للاتصالات ونظم المعلومات والمحافظة عليها من تهديدات الجرائم الأمنية على الانترنت، وبناء ثقافة آمنة ومحمية من جرائم تقنية المعلومات في دولة الإمارات العربية المتحدة. ويهدف فريق الاستجابة لطوارئ الحاسبات في الدولة إلى :

- تعزيز قانون مكافحة جرائم تقنية المعلومات والمساعدة في استحداث قوانين جديدة.
- تعزيز الوعي حول أمن المعلومات على مستوى الدولة.

(18) د.عبد الله عبد الكريم عبد الله: المرجع السابق، ص 94 وما بعدها. متوفر على الموقع www.eapiic.net

(19) د.علي حسن محمد الطوالبة: المرجع السابق، ص 94.

(20) د.عبد الله عبد الكريم عبد الله: المرجع السابق، ص 101- 102. متوفر على الموقع www.uaegroup.net

(21) نبيلة هبه هروال: المرجع السابق، ص 145.

(22) The united Arab emirates Computer Emergency Response Team

- بناء خبرات وطنية في مجال أمن المعلومات، وإدارة الطوارئ وتحري الأدلة في الحاسبات.
- إنشاء مركز اتصال موثوق للإبلاغ عن جرائم تقنية المعلومات في الدولة.
- إنشاء مركز وطني لجمع المعلومات عن التهديدات والمخاطر وجرائم تقنية المعلومات.
- تشجيع إنشاء ومساعدة فرق الاستجابة لحوادث أمن الحاسبات في القطاعات المختلفة.
- التنسيق مع الفرق المحلية والدولية للاستجابة لحوادث أمن الحاسبات والمؤسسات ذات الصلة.
- أن يصبح المركز عضواً فعالاً في المؤسسات والمنتديات الأمنية المعروفة.

ويقدم فريق امن المعلومات في الهيئة ثلاثون خدمة بين استباقية وتفاعلية تتدرج تحت أربعة أقسام وهي: رصد الهجمات الالكترونية والاستجابة لها، والأبحاث والتحاليل، والتوعية الأمنية، وخدمات جودة أمن المعلومات، ويتم إعطاء الأولوية للجهات الحكومية لطبيعة بناها التحتية.

وفي عام 2012 حققت دولة الإمارات العربية المتحدة في مجال الأمن الإلكتروني المرتبة الأولى إقليمياً والرابعة عالمياً، وذلك بحسب تقرير الكتاب السنوي للتنافسية الصادر عن المعهد الدولي للتنمية الإدارية[23].

ومن الجدير بالذكر أنه يوجد مثل هذا المركز في خمسة دول عربية أخرى، وهي عُمان وقطر والسعودية ومصر وتونس.

<u>5- سورية:</u>

نصت المادة 24 من قانون مكافحة الجريمة المعلوماتية على ما يلي :

(أ- تُحدث في وزارة الداخلية ضابطة عدلية مختصّة تكلَّف باستقصاء الجرائم المعلوماتية، وجمع أدلتها الرقمية، والقبض على فاعليها، وإحالتهم على المحاكم الموكول إليها أمر معاقبتهم.

ب- تستعين الضابطة العدلية المشار إليها في الفقرة (أ) من هذه المادة بخبراء، دائمين أو مؤقتين، من وزارة الدفاع، ووزارة العدل، ووزارة الاتصالات والتقانة، لتنفيذ المهام الموكلة إليها. ويقسم هؤلاء الخبراء اليمين القانونية.)

وتنفيذاً لهذا النص فقد أصدر السيد وزير الداخلية القرار 564/ ق تاريخ 2012/3/22 المتضمن إحداث فرع خاص في إدارة الأمن الجنائي يسمى (فرع مكافحة جرائم المعلوماتية) لمكافحة

([23]) متوفر على الموقع www.aecert.ae

هذه جرائم والتحقيق فيها، وجمع أدلتها الجنائية الرقمية، وضبط مرتكبيها وتقديمهم للقضاء. كما أصدر السيد وزير العدل القرار رقم 5413 تاريخ 2012/3/29 المتضمن تسمية قاضي كممثل لوزارة العدل في اللجنة المختصة بالتعاون مع هذا الفرع[24].

ثانياً– الأجهزة المختصة بمكافحة جرائم المعلوماتية على المستوى الدولي و الأوربي:

تتصف جرائم الإنترنت كما ذكرنا بأنها عابرة للحدود، ويمكن أن يتعدى أثرها عدة دول؛ لذلك كان لا بد من وجود تعاون دولي من أجل مكافحة هذا النوع من الإجرام. ومن أساليب التعاون الدولي، التعاون الشرطي الذي يمكن أن يحقق أهدافاً لا قِبلَ للشرطة الإقليمية بتحقيقها. ومن أبرز هذه الأجهزة في مجال مكافحة هذه الجرائم:

1–المنظمة الدولية للشرطة الجنائية (الإنتربول):

تعد هذه المنظمة من أهم الأجهزة على المستوى الدولي لمكافحة الإجرام بشكل عام، ومنها جرائم الإنترنت. وهي منظمة تتخذ مقراً لها في مدينة باريس. وتسعى هذه المنظمة لتحقيق التعاون المتبادل بين أجهزة الشرطة في مختلف الدول الأطراف، بهدف مكافحة الجرائم ذات الطابع العالمي، بما في ذلك الإجرام المرتبط بالإنترنت. وتستخدم هذه المنظمة وسيلتين لتحقيق أهدافها:

الأولى: تجميع البيانات والمعلومات المتعلقة بالجريمة والمجرم، عن طريق مكاتب هذه المنظمة الموجودة في أقاليم الدول الأعضاء.

والثانية: التعاون في ملاحقة المجرمين الفارين، وإلقاء القبض عليهم، وتسليمهم إلى الدول التي تطلب تسليمهم.

ولقد أنشأت هذه المنظمة وحدة متخصصة في مكافحة جرائم التكنولوجيا، كما تقوم بتزويد الشرطة في الدول الأطراف بكُتيبات إرشادية حول جرائم الإنترنت، وكيفية التدريب على مكافحتها والتحقيق فيها.

ومن بين إنجازات هذه المنظمة في مجال مكافحة جرائم الإنترنت، العملية التي قامت بها بالتعاون مع المباحث الفيدرالية الأمريكية FBI، والمتعلقة بملاحقة الهاكر الذي قام بإرسال فيروس الحب

(24) وقد سُمي المؤلف في هذا القرار ممثلاً عن وزارة العدل.

Love BUG عبر الإنترنت في الفلبين[25].

وإلى جانب الإنتربول، تقوم منظمة التعاون الاقتصادي والتنمية OECD[26] بمعالجة إشكاليات مواجهة جرائم الإنترنت.

كما قامت مجموعة الدول الثمانية الاقتصادية، وبالتعاون مع بعض المنظمات الدولية، وبعض الدول الأخرى مثل الصين ومصر، بتكوين قوة دولية أطلق عليها DOT FORCE[27]، و تهدف إلى تحقيق الأمن على شبكة الإنترنت[28].

2- مركز الشرطة الأوربية أو الأوروبول:

وهو جهاز على مستوى الاتحاد الأوربي، مقره في مدينة "لاهاي" بهولندا. وقد تم إنشاء الأوروبول من قبل المجلس الأوربي في لكسمبورغ عام 1991، ليكون بمثابة حلقة وصل بين الشرطة الوطنية في مختلف الدول الأعضاء، بهدف تسهيل عملية الملاحقة للجرائم العابرة للحدود.

وللأوروبول دور فعال في مكافحة جرائم الإنترنت، حيث يقوم مثلاً بالتحقيقات المتعلقة بامتلاك المواقع الإباحية ونشرها عبر الإنترنت في الدول الأوربية[29].

3-الأورجست:

وهو جهاز يعمل على المستوى الأوربي إلى جانب الأوروبول في مجال مكافحة جميع أنواع الجرائم، وينعقد اختصاصه عندما تمسّ الجريمة دولتين على الأقل من الدول الأعضاء في الاتحاد الأوربي، أو دولة عضو مع دولة من دول العالم الثالث، أو دولة عضو مع الرابطة الأوربية. ويشمل هذا الاختصاص الأفراد والمؤسسات على حدٍ سواء.

ويعد الأورجست بمثابة الدعامة الفعّالة في مجال التحقيقات والمطاردات التي تقوم بها السلطات

(25) نبيلة هبه هروال: المرجع السابق، ص 149 وما بعدها.

(26) وهو اختصار لـ Organization for Economic co-operation and Development

(27) وهو اختصار لـ Digital Opportunity Task Force

(28) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق، ص 814.

(29) د.جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، ص 79. نبيلة هبه هروال: المرجع السابق، ص 158.

القضائية الوطنية، وخصوصاً فيما يتعلق بجرائم الإنترنت[30].

4-شنجن:

إلى جانب الأوروبول والأورجست، تمّ إنشاء فضاء جماعي لا حدود له، أُطلق عليه اسم شنجن (Schengen)، وهو اسم مأخوذ من الاتفاقية الموقعة في عام 1985.

وقد استحدثت هذه الاتفاقية وسيلتين جديدتين لتعزيز التعاون الشرطي الأوربي في مواجهة التحديات الجديدة ومنها جرائم الإنترنت، وهاتان الوسيلتان هما: مراقبة المشتبه بهم عبر الحدود، وملاحقة المجرمين[31].

([30]) نبيلة هبه هروال: المرجع السابق، ص 159.

([31]) نبيلة هبه هروال: المرجع السابق، ص 161.

اختصاصات الضابطة العدلية في مكافحة جرائم المعلوماتية

يقوم موظفو الضابطة العدلية في سورية في الظروف العادية بمجموعة من الوظائف وهي: استقصاء الجرائم، وجمع الأدلة، وتلقي الإخبارات والشكاوى، وتنظيم المحاضر المتعلقة بهذه الجرائم[32]. وقد أشرنا سابقاً أن المادة 24 من قانون مكافحة الجريمة المعلوماتية قد أحدثت ضابطة عدلية مختصّة باستقصاء الجرائم المعلوماتية، وجمع أدلتها الرقمية، والقبض على فاعليها، وإحالتهم على المحاكم الموكول إليها أمر معاقبتهم.

ويقصد بالظروف العادية، جميع الأحوال التي يصل فيها إلى علم موظف الضابطة العدلية نبأ وقوع الجريمة، سواء عن طريق الإخبار أو الشكوى. ويخرج عن هذه الأحوال، الظروف الاستثنائية التي تتسع فيها صلاحيات موظفي الضابطة العدلية، كحالة الجرم المشهود، والجناية أو الجنحة الواقعة داخل مسكن، والإنابة.

وقد سمحت المادة 26 من قانون مكافحة الجريمة المعلوماتية، بالتقصي الإلكتروني، والتفتيش، والضبط حيث نصت على ما يلي :

(أ- يجوز للضابطة العدلية القيام بعمليات التقصي الإلكتروني، بناءً على إذن من السلطة القضائية المختصّة.

ب- تعدّ البرمجيات الحاسوبية من الأشياء المادية التي يجوز تفتيشها وضبطها، وفق القواعد المنصوص عليها في قانون أصول المحاكمات الجزائية.

ج- يجوز تفتيش الأجهزة والبرمجيات الحاسوبية المتصلة بأجهزة المشتبه فيه، أيّاً كان مكان وجودها، ضمن حدود الواقعة المسندة إلى المشتبه فيه.

د-على مقدّمي الخدمة على الشبكة الالتزام بالحفاظ على سرية الإجراءات التي تقوم بها الضابطة العدلية المختصّة في جميع الحالات.

هـ-على كل صاحب أو مدير أي منظومة معلوماتية تُرتكب جريمة معلوماتية باستخدام منظومته، أن يتيح للضابطة العدلية تفتيش وضبط البيانات والمعلومات والبرمجيات الحاسوبية، والحصول على نسخة منها؛ ويمكن في حالات الضرورة ضبط الأجهزة والبرمجيات الحاسوبية المستخدمة أو جزء

---

(32) المواد 14 حتى 27 من قانون أصول المحاكمات الجزائية.

من مكوّناتها.

و –يُعاقَب بالحبس من شهر إلى ستة أشهر والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية، كل من يخالف أحكام هذه المادة.)

وسنتناول اختصاصات هذه الضابطة كما يلي :

أولاً– تقديم الإخبار أو الشكوى عن جرائم المعلوماتية:

لا تختلف أحكام الإخبار أو الشكوى في جرائم المعلوماتية كثيراً عن ما هو عليه الحال في الجرائم التقليدية. فمن الممكن أن يتم الإخبار عن جرائم المعلوماتية **بالأسلوب المادي**، كأن يتوجه مقدم الإخبار بنفسه إلى أقرب قسم للشرطة أو للنيابة العامة للإدلاء ببلاغه. كما يمكن أن يتم الإخبار **بالأسلوب المعنوي** عن طريق الهاتف أو البريد العادي.

وإلى جانب هذين الأسلوبين، ظهر أسلوب ثالث في إطار جرائم المعلوماتية وخاصة جرائم الإنترنت، وهو **الأسلوب الرقمي**، حيث أصبح من الممكن تقديم الإخبار أو الشكوى عن طريق الإنترنت بإحدى الطريقتين التاليتين:

الطريقة الأولى: وهي كتابة رسالة إلكترونية تتضمن الإبلاغ عن جريمة إنترنت، وإرسالها إلى عنوان البريد الإلكتروني العائد لأحد الأجهزة المختصة بمكافحة جرائم الإنترنت، كالقيام بكتابة رسالة إلكترونية تتضمن الإخبار عن وجود مواقع إلكترونية أُعدت للاحتيال أو مواقع إباحية مثلاً، وإرسالها إلى عنوان البريد الإلكتروني للجهة المختصة، كموقع المباحث الفيدرالية الأمريكية FBI، أو موقع إدارة العدل الأمريكية USDJ، أو موقع وكالة المخابرات المركزية الأمريكية CIA، أو موقع هيئة حماية البرمجيات الأوربية APP، أو غيرها من المواقع الأخرى[33].

الطريقة الثانية: وهنا يتم التبليغ عن طريق ملء بيانات الاستمارة الرقمية، التي تكون متوفرة عادةً على المواقع الإلكترونية المخصصة لتلقي الإخبارات والشكاوى، كما هو متبع في المواقع التالية[34]:

- الموقع الإلكتروني لمركز تلقي شكاوى جرائم الإنترنت IC3[35].

(33) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق، ص 825.

(34) نبيلة هبه هروال: المرجع السابق، ص182.

(35) www.IC3.gov

- الموقع الإلكتروني لمركز جرائم الياقات البيضاء NW3C[36].

- موقع إدارة مكافحة جرائم الحاسبات وشبكات المعلومات، العائد للحكومة المصرية[37].

- الموقع الإلكتروني العائد للمكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصالات في فرنسا. فبعد أن يتم تلقي البلاغات عن طريق هذا الموقع الفرنسي، تتم عملية تحليل ودراسة تلك البلاغات، للتأكد من صحة ما ورد فيها من معلومات حول واقعة الجريمة، ثم يتم إبلاغ مصالح الدرك والشرطة حسب الاختصاص الإقليمي؛ كما يتم إعطاء مقدم الإخبار رقم الاستمارة الرقمية الخاصة به حتى يتمكن من معرفة مستجدات التحقيقات[38].

و لابدّ من الإشارة إلى الدور الهام الذي يلعبه مقدم الإخبار أو الشاكي في إطار جرائم الإنترنت، لأنه في كثير من الأحيان يكون هذا الإخبار هو الوسيلة الوحيدة لعلم السلطات المختصة بوقوع الجريمة.

ومما تقدم، نجد أن تقديم الإخبار أو الشكوى عبر الإنترنت يسّهل عملية إعلام السلطات المختصة بوقوع الجريمة، كما يؤمّن الحماية لمقدم الإخبار الذي يظلّ مجهولاً في أغلب الأحيان. لذلك نقترح على أجهزة العدالة السورية أن تنشأ مواقع إلكترونية متخصصة في تلقي الإخبارات والشكاوى المتعلقة بجرائم المعلوماتية.

ثانياً– استقصاء الجرائم وإثباتها:

إن **الواجب الأول** الذي يقع على عاتق الضابطة العدلية هو استقصاء الجرائم، أي التحري عنها. فالاستقصاء هو البحث عن جريمة لم يثبت بعد وقوعها فعلاً، إما بناء على شكوى أو إخبار، أو بناء على تكليف من النيابة العامة، أو بناء على معلومات وصلت إلى رجل الضابطة العدلية من أي مصدر كان.

أما **الواجب الثاني**، وهو إثبات الجرائم، فيقصد به جمع الأدلة على وقوع الجريمة، ومعرفة مرتكبها والقبض عليه. والسرعة بجمع الأدلة يساعد على المحافظة على آثار الجريمة، وإحكام الطوق

---

(36) www.NW3C.org

(37) www.ccd.gov.eg .

(38) نبيلة هبه هروال: المرجع السابق، ص187، وعنوان الموقع الفرنسي هو: www.internet-mineurs.gov

على الجاني[39].

ولرجال الضابطة العدلية في سبيل قيامهم بهذين الواجبين أن يسلكوا كل السبل المجدية لكشف الجريمة؛ فالقانون لم يحدد شكلاً خاصاً لاستقصاء الجرائم وجمع أدلتها، لذلك كان من حقهم أن يستعينوا بكل الوسائل المشروعة للتحري عن الجرائم، دون انتظار توجيه أمر لهم بذلك من رؤسائهم.

ولكن يجب على رجال الضابطة العدلية عدم اللجوء إلى الغش أو الخديعة من أجل الحصول على الأدلة، فلا تثريب عليهم إذا استعملوا بأي وسيلة بارعة لا تتصادم مع الأخلاق، مثل التخفي، وانتحال الصفات، واصطناع المرشدين. فيمكن لرجل الضابطة العدلية أن يتظاهر بأنه مدمن مخدرات ويرغب في شراء كمية منها ليقبض على المروج. ولكن ليس له أن يخلق الجريمة من العدم، كأن يدفع الفاعل إلى ارتكابها، ثم يلقي القبض عليه، لأنه في ذلك لا يكتشف الجريمة بل يوجدها. والقانون لم ينظم قواعد التحري، لذلك يبقى الأمر اجتهاداً، غير أنه يجب ألاّ يخالف القواعد الدستورية أو القانونية[40].

ومن المؤكد أن قيام رجال الضابطة العدلية بأعمال الاستقصاء وإثبات الجرائم، إنما يهدف إلى مساعدة النيابة العامة على اتخاذ قرارها بتحريك الدعوى العامة أو عدم تحريكها؛ فإذا قامت بتحريكها، وجب عليهم أن يتوقفوا عن العمل من تلقاء أنفسهم، ولا يجوز لهم أن يباشروا أي عمل من أعمال الضابطة العدلية إلاّ إذا كلفهم قاضي التحقيق بذلك بموجب قرار ندب[41].

وإجراءات استقصاء الجرائم تعدّ من الأهمية بمكان، سواء أكانت الجرائم تقليدية أم مستحدثة . وفي إطار جرائم الإنترنت، فإن أبرز وسائل الاستقصاء وجمع الأدلة هي: وسيلة الإرشاد الجنائي، ووسيلة المراقبة الإلكترونية. وهذا ما سنتناوله على التتالي:

أ-الإرشاد الجنائي عبر الإنترنت:

يعدّ الإرشاد الجنائي من أهم الوسائل التي يمكن أن يعتمد عليها رجال الضابطة العدلية في عملية تحري واستقصاء جرائم الإنترنت.

ويقصد بالإرشاد الجنائي قيام عنصر الضابطة العدلية أو الغير، بالولوج إلى الإنترنت، والدخول في حلقات النقاش والدردشة، مستخدماً اسماً أو صفةً مستعارة أو وهمية، وذلك بقصد البحث عن الجرائم

([39]) د.عبد الوهاب حومد: أصول المحاكمات الجزائية، الطبعة الرابعة،المطبعة الجديدة، دمشق، 1990، ص 100.

([40]) د.عبد الوهاب حومد: أصول المحاكمات الجزائية،المرجع السابق، ص 101-103.

([41]) د.عبد الوهاب حومد: أصول المحاكمات الجزائية،المرجع السابق، ص 100.

ومرتكبيها، وإلقاء القبض عليهم، وإحالتهم إلى القضاء[42].

والفارق بين نظام الإرشاد الجنائي في الجرائم التقليدية ونظام الإرشاد الجنائي في جرائم الإنترنت، هو أن المرشد أو المخبر في الجرائم التقليدية غالباً ما يكون من الغير، أي ليس من رجال الضابطة العدلية، أما المرشد في جرائم الإنترنت، فمن الممكن أن يكون أحد رجال الضابطة العدلية، إذ إن الأمر لا يتطلب منه سوى الحصول على إذن رسمي من رؤسائه للقيام بهذه المهمة، ثم يلج بواسطة حاسوبه إلى شبكة الإنترنت، حيث يدخل إلى حلقات الدردشة والنقاش مثلاً، مستخدماً اسماً مستعاراً أو صفة وهمية، فيتناول الأحاديث العادية مع الغير، دون أن يدفعه إلى ارتكاب الجريمة، فيظهر وكأنه يسعى لإضاعة الوقت والهروب من الملل، إلى أن يبرز هذا الغير مشروعه الإجرامي، كأن يدور الحديث حول طريقة الحصول على أرقام بطاقات الائتمان بصورة احتيالية، أو كيفية إعداد المواقع الخلاعية،أو المواقع المعدة لبيع المسروقات، أو كيفية اختراق المواقع، أو زرع الفيروسات...الخ. ويمكن للمرشد أيضاً أن يقوم بطرح الأسئلة على الغير، حتى يتمكن من الحصول على أكبر قدر ممكن من المعلومات، وعندما تتضح الصورة كاملةً، يقوم المرشد -إذا كان من الغير- بإيصال هذه المعلومات إلى الجهات المختصة، التي تباشر عملها في تعقب هذا المجرم والقبض عليه، مستخدمة في ذلك برمجيات معينة تقودها إلى مزود خدمة الإنترنت الذي يتحرك فيه هذا المجرم؛ أما إذا كان المرشد أحد رجال الضابطة العدلية، فيقوم باستدراج المجرم حتى يتم القبض عليه[43].

ومن أمثلة الإرشاد الجنائي، قيام مكتب التحقيقات الفيدرالي FBI، بضبط أفراد عصابة "فاستلان" Fastlan المنتشرين حول العالم، الذين امتهنوا قرصنة البرمجيات وتحميلها على مواقع للهكرة، وجنوا أرباحاً وصلت إلى مليون دولار في فترة زمنية قصيرة، حيث تم إلقاء القبض على تسعة منهم في الولايات المتحدة الأمريكية، وتمّت إدانتهم أمام هيئة المحلفين العليا في شيكاغو. وقد استعملت المباحث الفيدرالية في هذه القضية أسلوب الإرشاد الجنائي، عندما دسّت أحد عناصرها في هذه العصابة إلى أن تمّ إلقاء القبض عليهم[44].

وفي مثال آخر، فقد قام المدعو Roots أثناء وجوده في إحدى حلقات الدردشة عبر الإنترنت بالتحدث مع فتاة لم تتجاوز الرابعة عشرة من عمرها في موضوعات جنسية؛ وتناول الحديث عرضه لها

(42) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق،ص 838.

(43) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق، ص 838- 839.

(44) د.سليمان أحمد فضل: المرجع السابق، ص 275.

ممارسة الأفعال الجنسية معها، وتمّ تحديد موعد اللقاء بينهما في أحد المتاجر؛ وعندما وصل تمّ القبض عليه، إذ تبين أن الفتاة الصغيرة لم تكن سوى أحد أعضاء فريق مكافحة الجريمة عبر الإنترنت، في حالة تنكر بهيئة فتاة صغيرة بتكليف من الإدارة التي تعمل فيها(45).

والحقيقة أن نظام الإرشاد الجنائي عبر الإنترنت هو من أهم وسائل تحري واستقصاء جرائم الإنترنت، وهو نظام لا بدّ من الأخذ به في جميع الدول التي تسعى للحدّ من هذه الجرائم.

ب- التقصي الإلكتروني أو المراقبة الإلكترونية Electronic Surveillance:

يقصد بالتقصي الإلكتروني أو المراقبة الإلكترونية "ذلك العمل الذي يقوم به المراقب، باستخدام التقنية الإلكترونية، لجمع المعلومات عن المشتبه به، سواء أكان شخصاً أم مكاناً أم شيئاً، وذلك لتحقيق غرض أمني" (46).

فالمشتبه به الإلكتروني يمكن أن يكون شخصاً، أو موقعاً، أو بريداً إلكترونياً مخالفاً للقانون. وتشمل المراقبة الإلكترونية جميع تحركات المشتبه به عبر الإنترنت، بما في ذلك بريده الإلكتروني.

ويشترط في المراقبة الإلكترونية أن تكون مشروعة. والغرض من هذه المشروعية هو تحقيق نوع من التوازن بين حق الأفراد في الخصوصية، وحق المجتمع في مكافحة الجريمة بوسائل فعّالة حفاظاً على أمنه. وعلى ذلك فيمكن لرجل الضابطة العدلية أن يقوم طبقاً للقانون بمراقبة أحد الهكرة أثناء اختراقه لحاسوب المجني عليه، أو أن يراقب أحد المواقع التي أُعدت للاحتيال على الناس...الخ.

ومن الملاحظ أن معظم الدول أخذت بنظام المراقبة الإلكترونية ضمن شروط معينة، بهدف رصد الجرائم المستحدثة. **ففي الولايات المتحدة الأمريكية**، نظّم قانون خصوصية الاتصالات الإلكترونية ECPA(47) كيفية حصول أجهزة العدالة على المعلومات المخزنة في مُخدّمات مزودي خدمة الإنترنت، فأعطى الحق لرجل الضبط القضائي في الحصول على المعلومات الأساسية للمشترك (كالاسم والعنوان وغيرها)، أو المعلومات المتعلقة ببريده الإلكتروني أو بريده الصوتي، بمجرد توجيه أمر من المحكمة إلى

---

(45) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق، ص276.

(46) د.مصطفى محمد موسى: المراقبة الإلكترونية عبر شبكة الإنترنت (دراسة مقارنة)، سلسلة اللواء الأمنية في مكافحة الجريمة الإلكترونية، العدد الخامس، مطابع الشرطة للطباعة والنشر والتوزيع، القاهرة،2003، ص192.

(47) وهو اختصار لـ The Electronic Communication Privacy Act وقد تمّ تعديله بموجب القانون الوطني الأمريكي Patriot Act 2001، ومتوفر على الموقع: www.wikipedia.org

مزود خدمة الإنترنت تأمره فيه بالكشف عن محتويات الحساب[48].

أما الاتفاقية الأوربية حول الجريمة الافتراضية لعام 2001، فقد سمحت المادتان /20 / و /21/ منها بمراقبة حركة البيانات ومحتواها أثناء عملية التراسل[49].

وفي فرنسا، أصدر المشرع الفرنسي القانون المؤرخ في 2000/8/1، الذي عدّل قانون حرية الاتصالات المؤرخ في 1986/9/30، حيث سمح بمقتضى هذا التعديل لمزودي الخدمات بمراقبة حركة أعضاء الإنترنت[50].

وفي هولندا، يجوز لقاضي التحقيق أن يأمر بالتنصت على شبكات الاتصالات الحاسوبية، إذا كانت هناك جرائم خطيرة ارتكبها المتهم[51].

و في سورية فقد سمحت الفقرة أ من المادة 26 من قانون مكافحة الجريمة المعلوماتية بالتقصي الإلكتروني أو المراقبة الإلكترونية **بشرط الحصول على إذن من السلطة القضائية المختصة**، ويشمل مفهوم السلطة القضائية النيابة العامة وقضاء التحقيق والمحاكم الجزائية.

والسؤال المطروح هنا هو: **ما هي التقنية المستخدمة في المراقبة الإلكترونية؟**

تعددت التقنيات المستخدمة في مجال المراقبة الإلكترونية، فهناك برامج مخصصة لفحص الرسائل الإلكترونية الصادرة والواردة، وبرامج تقوم باستعادة الرسائل التي تمّ إلغاؤها أو محوها، وأخرى تقوم بتعقب المواقع الإباحية، وغير ذلك من هذه البرمجيات. وسنتناول فيما يلي أبرز أنواع هذه البرمجيات:

1- تقنية برنامج "كارنيفور" للتنصت على البريد الإلكتروني:

طورت إدارة تكنولوجيا المعلومات التابعة لمكتب التحقيقات الفيدرالي FBI، برنامج أطلق عليه اسم "كارنيفور"، حيث يقوم هذا البرنامج بتعقب وفحص رسائل البريد الإلكتروني الصادرة والواردة عبر المخدمات المستخدمة من قبل مزودي خدمة الإنترنت، إذا كان هناك اشتباه بأن هذه الرسائل تحمل معلومات عن جرائم أو حوادث جرمية. فهذا البرنامج يقوم بفحص وتسجيل الرسائل التي تحتوي كلمات

(48) د.عمر بن يونس: الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي،المرجع السابق، ص 271 .

(49) د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية، المرجع السابق ص161.

(50) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق، ص 202.

(51) د.علي حسن محمد الطوالبة: المرجع السابق، ص 150.

أو معلومات يشتبه في أن لها علاقة بالجرائم، ويتجاهل الرسائل الأخرى[52].

2- برامج استعادة الوثائق الإلكترونية الممحاة:

في عام 1988، أسس الأمريكي "جون جيسين" شركة تدعى "اكتشاف الأدلة أو القرائن الإلكترونية". وقد اتجهت هذه الشركة لتسهيل عملها في البحث والتحري نحو الوثائق الإلكترونية، باعتبار أن هذه الوثائق تترك وراءها أثراً لا يُمحى، ويمكن استعادتها مهما اجتهد الفاعل في محوها، وذلك على عكس الوثائق الورقية التي تتحول إلى مادة يصعب استرجاع المعلومات منها بعد حرقها أو تمزيقها.

وقد طورت هذه الشركة العديد من برامج البحث في ذاكرة الحاسوب عن الرسائل الممحاة والمعلومات المصاحبة لها، وهذه المعلومات تشمل الطريق الذي سلكته الرسالة والمرفقات التي أُرسلت معها، وأجهزة الحاسوب التي مرت بها، فكأن هذا البرنامج يخرج الحي من الميت.

و من أشهر القضايا الذي اعتمدت على هذا الأسلوب، القضية التي رفعتها وزارة العدل الأمريكية وتسع عشرة ولاية ضد شركة مايكروسوفت، لمحاولتها احتكار أنظمة تصفح الإنترنت. فبعد البحث في نظام البريد الإلكتروني العائد لهذه الشركة، تم اكتشاف رسائل إلكترونية تتعلق بمحاولة الإضرار بالمنافسين التجاريين، التي اعتقد أصحابها أنهم قاموا بمحوها. ومن أشهر الرسائل الممحاة التي استخدمت في هذه القضية، الرسالة التي سأل فيها رئيس مايكروسوفت عدداً من كبار الموظفين في شركته عمّا إذا كان لديهم خطة تتعلق بما يمكن فعله من أجل إلحاق الضرر بالخصوم التجاريين[53].

3- برنامج مراقبة البريد الإلكتروني:

وهو برنامج صمّمه المبرمج الأمريكي "ريتشارد إتوني"، حيث يقوم هذا البرنامج بسبر محتوى البريد الإلكتروني موضوع المراقبة، وقراءة الرسائل التي قام صاحبها بإتلافها، أو تلك التي لم يقم بتخزينها أصلاً، ويمكن تحميل هذا البرنامج على أي جهاز حاسوب بهدف مراقبة بريده الإلكتروني. وقد استخدمت المخابرات الأمريكية هذا البرنامج لكشف مشتبه به من الجنسية الروسية حاول اختراق بعض المواقع على شبكة الإنترنت[54].

---

(52) د.مصطفى محمد موسى: دليل التحري عبر شبكة الإنترنت، دار الكتب القانونية، القاهرة، ص 189.

(53) د.مصطفى محمد موسى: دليل التحري عبر شبكة الإنترنت، المرجع السابق ص 193-194.

(54) د.مصطفى محمد موسى: المراقبة الإلكترونية عبر شبكة الإنترنت، المرجع السابق ص216.

4- برنامج تعقب المواقع الإباحية:

ويعرف هذا البرنامج باسم "نوبد شرطة الإنترنت" وهو يقوم بالبحث عن الصور الجنسية المخلّة بالأخلاق في أنظمة الحواسيب التي تعمل وفق برنامج تشغيل ويندوز بإصداراته الحديثة، ثم يقوم بتبليغ الهيئات الحكومية عنها، بهدف تطهير شبكة الإنترنت من هذه المواقع والصور[(55)].

ومن الأمثلة الشهيرة للمراقبة الإلكترونية، أنه تمّ الكشف عن العلاقة الغرامية بين الرئيس الأمريكي السابق "كلينتون" والآنسة "مونيكا لوينسكي"، عن طريق مراقبة البريد الإلكتروني لهما[(56)].

ثالثاً- القبض:

القبض هو" إمساك الشخص من جسمه، وتقييد حركته وحرمانه من حق التجول، دون أن يتعلق الأمر على فترة زمنية معينة ." [(57)]

والقبض بطبيعته إجراء ماس بالحرية الشخصية، التي هي حق أساسي للإنسان، ولذلك حرص الدستور على حمايتها، وفصّل القانون في ضوابط هذه الحماية[(58)]. فقانون أصول المحاكمات الجزائية لم يجز القبض على أحد إلا في حالتين فقط، هما[(59)] :

1- الجرم المشهود (جناية مشهودة أو جنحة مشهودة).

2- وجود أمر من قاضي التحقيق، في حالات الجنايات والجنح غير المشهودة .

وفي إطار جرائم المعلوماتية، فالسؤال الذي يطرح نفسه هنا هو: **كيف يتم تعقب المشتبه به في جرائم الإنترنت ؟ بمعنى أخر، كيف يتم القبض على مجرم الإنترنت؟**

للإجابة عن هذا السؤال سنلقي الضوء على آلية تعقب المشتبه به في جرائم الإنترنت، ثم نتعرض لأشهر الشركات التي تقوم بعملية التتبع، ومن ثم معرفة كيفية تتبع البريد الإلكتروني المزيف.

---

(55) د.مصطفى محمد موسى: المراقبة الإلكترونية عبر شبكة الإنترنت، المرجع السابق ص217.

(56) Eoghan Casey, op-cit, P-41.

(57) د.عبد الوهاب حومد: أصول المحاكمات الجزائية،المرجع السابق، ص 125.

(58) د.محمود نجيب حسني: شرح قانون الإجراءات الجنائية،المرجع السابق، ص 556.

(59) المواد 29 و112 و231 و102 حتى 116 من قانون أصول المحاكمات الجزائية . د.عبد الوهاب حومد: أصول المحاكمات الجزائية،المرجع السابق، ص 123.

2- آلية تعقب المشتبه به في جرائم الإنترنت:

تتيح البنية التحتية للإنترنت إمكانية التعرف على عنوان الحاسوب المستخدم في ارتكاب الجريمة فقط، وهو ما يعرف بعنوان Internet Protocol (IP)، الذي يشير إلى رقم يتم بموجبه تحديد الحاسوب الذي تمّ النفاذ من خلاله إلى الإنترنت. وبعد تحديد هوية الحاسوب المستخدم بارتكاب الجريمة، تبدأ عملية اتخاذ الإجراءات اللازمة لإلقاء القبض على المشتبه به[60].

ويمكن تشبيه عنوان الإنترنت الرقمي IP Address بأرقام الهواتف. فعنوان الإنترنت يزودنا بالمنطقة الجغرافية التي انطلقت منها الرسالة (البلد والمدينة، واسم المضيف Hostname، وتحديد الموقع التقريبي)، وبفضل هذه المعلومات يمكن في أغلب الأحوال تعيين المشتبه به[61].

وعنوان الإنترنت الرقمي يمكن الحصول عليه عن طريق مزود خدمة الإنترنت، إذ إن مزود الخدمة يقوم بالحصول على مجموعة كبيرة من العناوين عن طريق الجهات المسؤولة جغرافياً عن إدارة وتخصيص هذه العناوين. فمثلاً الريب RIPE NCC[62] وهي إحدى الجهات المرخص لها من قبل الآيكان ICANN، تقوم بتخصيص عناوين النفاذ لمنطقة أوربا والشرق الأوسط وبعض دول آسيا وإفريقيا. وسورية تنتمي إلى هذه المنطقة حسب ترتيبات الآيكان، وتدير المؤسسة العامة للاتصالات في سورية حالياً النطاق العلوي السوري، حيث تقوم بتخصيص أسماء النطاقات الداخلية للراغبين في الحصول عليها لقاء رسوم سنوية.

أما تخصيص عناوين الإنترنت فيتم بطريقتين، هما[63]:

الطريقة الأولى: ثابتة Statically. ووفقاً لهذه الطريقة يتم تخصيص عنوان محدد للمشترك عن طريق مزود خدمة الإنترنت. فعلى سبيل المثال، لو أن مزود الخدمة حصل على /1000/ عنوان رقمي عن طريق الجهات المسؤولة، وأراد تخصيص هذه الأرقام لزبائنه بالطريقة الثابتة، فإن إجمالي عدد هؤلاء الزبائن سيكون /1000/ مشترك.

---

(60) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق، ص 811.

(61) www.WhatIsMyIPAddress.com وهو موقع مخصص للتعرف على بروتوكول الـ IP.

(62) وهو اختصاص لـ Reseau IP Europeans Network Coordination Center ومتوفر على الموقع www.ripe.net

(63) Anthony Reys and others, Cyber Crime Investigations, Bridging The Gaps Between Security Professional Law, Enforcement and Prosecutors. Published by Elsevier Since and Technology, 2007, P-200-201.

الطريقة الثانية: متحركة أو ديناميكية Dynamically. وفي هذه الحالة لا يتم تخصيص زبائن مزود خدمة الإنترنت بعناوين محددة. فمثلاً عندما يريد المشترك الدخول إلى الإنترنت، فإنه يطلب ذلك عن طريق مزود الخدمة المشترك معه، حيث يكون لدى هذا المزود مُخدّم يسمى DHCP(64)، وهو عبارة عن حاسوب يحتوي على قائمة من العناوين الرقمية المتاحة، بحيث يمنح هذا المُخدّم أحدها للمشترك بشكل ديناميكي.

ومن الملاحظ أن مزود خدمة الإنترنت يعلم أن جميع المشتركين لديه لن يدخلوا إلى شبكة الإنترنت في نفس الوقت، لذلك يلجأ في الغالب إلى إتباع الطريقة الديناميكية، التي تؤمّن له مضاعفة عدد زبائنه، وتؤدي إلى تخفيض كلفة الحصول على العناوين الرقمية، ومن ثم تحقيق عائدات مالية أكبر.

وتجدر الإشارة إلى أن بروتوكول الإنترنت المشار إليه، الذي يحدد هوية الحاسوب، لا يتم منحه بطريقة واحدة على المستوى العالمي. ففي الولايات المتحدة الأمريكية وكندا وبعض الدول المتقدمة، يقوم الشخص باقتناء IP خاص به، ومن ثم يمكن تحديد هويته بسهولة عند ارتكابه جريمة إنترنت. أما في بعض الدول الأخرى –ومنها أغلب الدول العربية– فإن العنوان الرقمي يكون محلاً للتغير بين عدة مشتركين، وبالتالي فإن تحديد هوية المشتبه به تكون أكثر صعوبة(65). ويمكن القول إنه بمجرد وجود شخص في سورية على الإنترنت، فإنه يملك فوراً هوية رقمية محددة IP، إلاّ أنه إذا حدث وانقطع الإرسال، فإن الشخص إذا عاود الاتصال من جديد، فإن الهوية السابقة قد لا تبقى له، بل لغيره، وقد يظهر بهوية جديدة، أي بـ IP جديد.

كما تجدر الملاحظة بأن الشبكات الداخلية تعد من الأمور الشائعة في مجال الشركات، حيث يحتاج العاملون في هذه الشركات إلى التواصل وتبادل الملفات فيما بينهم. ويمكن استخدام عنوان خارجي واحد لتشغيل عدد من الحواسيب المرتبطة فيما بينها عن طريق شبكة داخلية(66).

وفي حال ارتكاب جريمة إنترنت، عن طريق أحد الحواسيب الموصولة إلى شبكة داخلية، فإن على موظف الضابطة العدلية أن يتوصل إلى رقم العنوان الخارجي، ثم يتم تحديد الحاسوب المطلوب

---

(64) وهو اختصار لـ Dynamic Host of Configuration، ويعني بروتوكول التشغيل الديناميكي.

(65) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق، ص 811.

(66) Anthony Reys and others, op-cit, P-203.

عن طريق العنوان الداخلي، ومن ثم يتم معرفة الشخص المقصود.

ب-أشهر الشركات المختصة بعملية التتبع عبر الإنترنت:

قامت العديد من الشركات المختصة في مجال التكنولوجيا بتقديم نسخٍ متطورة من التقنيات التي تقوم بتحديد الموقع الجغرافي للمستخدم.

ومن أشهر هذه الشركات شركة Akamai، وهي شركة تقدم خدمة Edge Shape لزبائنها، بحيث تسمح هذه الخدمة بتتبع المستخدم عبر الإنترنت، وتحديد موقعه الجغرافي، عن طريق رسم خريطة للعنوان الرقمي العائد لهذا المستخدم، ثم يتم جمع هذه المعلومات في قاعدة بيانات على موقع الشركة الإلكتروني، بحيث تصبح متاحة لزبائنها.

فإذا اشترك مالك أحد المواقع الإلكترونية في خدمة Edge Shape، فإن أي شخص يقوم بالدخول إلى هذا الموقع في أي وقت، يتم جمع بيانات تفصيلية عنه، مثل البلد الذي تمّ الدخول منه، والموقع الجغرافي في هذا البلد، واسم مزود الخدمة الذي دخل من خلاله.

ومن الشركات التي تعمل في نفس المضمار أيضاً شركة Quova، وهي شركة مقرها "كاليفورنيا"، وقد طورت هذه الشركة خدمة Geopoint، حيث تصل دقة هذه الخدمة في تحديد متصفحي الإنترنت ومواطنهم ومواقعهم إلى نسبة 85% وحتى 98%. وقد استخدمت شركة Cinema Now المحدودة المسؤولية خدمة Geopoint، وهي شركة مقرها في "كاليفورنيا"، وتعمل في مجال توزيع الأفلام السينمائية عبر الإنترنت، من أجل حماية حقوقها على هذه الأفلام، والتأكد من أن عملية التوزيع تتم وفق الاتفاقيات القانونية للتوزيع والنشر (67).

ج- تتبع البريد الإلكتروني المزيف:

يقوم بعض المجرمين بتزييف أو تزوير البريد الإلكتروني، بغية إخفاء هويتهم الحقيقية. وكثيراً ما تخفق هذه المحاولات في إخفاء الهوية؛ لأن الرسائل المزيفة أو المزورة تحتوي على عناوين الإنترنت العائدة للمرسلين. ومن الملاحظ أن معظم المجرمين عبر الإنترنت يستخدمون هذا الأسلوب لإخفاء هويتهم الحقيقية.

ولمعرفة كيفية التلاعب بعناوين الإنترنت، لا بدّ لنا من التعرف على الآلية التي تتم بها عملية

---

(67) Adam D Thierer , op-cit, P-114 .

إرسال الرسائل الإلكترونية. فالبريد الإلكتروني يشبه البريد العادي في العديد من الجوانب. فعندما يتم إرسال رسالة إلكترونية، يقوم وكيل نقل الرسائل MTA[68]– وهو يشبه مكتب البريد العادي– بختم هذه الرسالة مع وضع وقت الإرسال، واسم وكيل نقل الرسائل، ومعلومات تقنية أخرى، وتكون هذه المعلومات موجودة في ترويسة الرسالة الإلكترونية، ويتم وضع هذه المعلومات من قبل جميع وكلاء نقل الرسائل التي تمرّ الرسالة الإلكترونية عبرهم، إلى أن تصل إلى الجهة المقصودة.

ومن أجل إخفاء عناوين الإنترنت، يقوم مزيفو البريد الإلكتروني بإدخال عناوين وهمية إلى ترويسة الرسالة الإلكترونية لتضليل المحققين، التي تحوي عادة على عناوين المُخدّمات التي مرّت عبرها الرسالة كما ذكرنا. إلاّ أن الخبير التقني يستطيع عن طريق التدقيق الجيد اكتشاف عدم التناسق بين العنوان الوهمي وباقي العناوين الصحيحة في ترويسة الرسالة. ناهيك عن أن الرسالة الإلكترونية ستحمل كحد أدنى العنوان الصحيح الذي تمّ من خلاله إرسال الرسالة الإلكترونية[69].

ومما تقدم نجد أنه من الأهمية بمكان توفير الأجهزة التقنية والخبرات الفنية لدى موظفي الضابطة العدلية، حتى يتمكنوا من تتبع الأثر الافتراضي للجاني، وتحديد مكانه وإلقاء القبض عليه.

رابعاً– التفتيش:

يعدّ التفتيش من أخطر الإجراءات التحقيقية لأنه يمسّ السر الخاص بالأشخاص؛ ولذلك تضمنت أغلب دساتير العالم مبدأ المحافظة على الأسرار الخاصة بالأشخاص. وقد تضمّن قانون العقوبات السوري نصوصاً تعاقب على خرق حرمة المنزل وعلى إفشاء الأسرار[70].

أ–تعريف التفتيش:

هو: "الاطلاع على محل منحه القانون حماية خاصة، باعتباره مستودع سر صاحبه، ويستوي في ذلك أن يكون المحل مسكناً أو ما هو في حكمه أو أن يكون شخصاً"[71]. والتفتيش كإجراء، هو في الأصل من اختصاص سلطة التحقيق الابتدائي، إلاّ أنه استثناءً يدخل في صلاحية موظفي الضابطة العدلية في الأحوال التي عيّنها القانون.

---

(68) وهو اختصار لـ Message Transfer Agents ويقصد به الحاسوب أو المخدم المسؤول عن نقل الرسائل الإلكترونية.

(69) Eoghn Casey: op-cit, P-465,466 .

(70) المواد 557 و 558 و 565 وحتى 567 من قانون العقوبات.

(71) يعود هذا التعريف إلى الدكتور أحمد فتحي سرور، نظرية البطلان في قانون الإجراءات الجنائية، رسالة دكتوراه، جامعة القاهرة،دار النهضة العربية– القاهرة، ص 449. مشار إليه عند د.علي الطوالبة: المرجع السابق، ص10.

ب-محل التفتيش:

لا يرد التفتيش إلا على الأسرار الخاصة. فالاطلاع على الأشياء المعلنة للجمهور لا يعدّ تفتيشاً، لأن محل التفتيش هو مستودع السر، ومن ثم فالتفتيش يمكن أن يرد على الشخص ذاته، أو على مكانه الخاص كالمنزل وملحقاته(72).

أما محل التفتيش في جرائم المعلوماتية، فيرد على ما يلي:

2- **المكونات المعنوية للحاسوب(البرمجيات):**

الحاسوب هو وسيلة النفاذ إلى العالم الافتراضي، وتشمل المكونات المعنوية للحاسوب، الأنظمة الأساسية كأنظمة التشغيل، والكيانات المنطقية التطبيقية كالبرامج التي تستخدم للقيام بعمل معين، و البيانات المخزنة في الحاسوب بأنواعها(73).

وقد قامت بعض الدول الأجنبية بسنّ تشريعات إجرائية حديثة، قنّنت فيها موضوع تفتيش مكونات الحاسوب البرمجية وضبطها. **ففي الولايات المتحدة الأمريكية**، نظم المشرع الأمريكي إجراءات تفتيش وضبط المكونات البرمجية للحاسوب، من خلال القوانين الإجرائية الفيدرالية المتعلقة بجرائم الحاسوب المنصوص عليها في القسم 42usc 2000(74).

أما الاتفاقية الأوربية حول الجريمة الافتراضية لعام 2001، فقد نظّمت تفتيش وضبط البيانات المخزنة في الحاسوب بالمادة 19 من هذه الاتفاقية.

أما في **المملكة المتحدة**، فقد سمح المشرع بتفتيش الحاسوب، بالقسم الرابع عشر من قانون إساءة استخدام الكمبيوتر لعام 1990، وذلك بعد الحصول على إذن بالتفتيش من القاضي المختص(75).

وفي بلجيكا، أصدر المشرع البلجيكي القانون المؤرخ بـ 2001/11/28 المتضمن تعديل قانون التحقيق الجنائي، الذي أضاف المادة /88/ إلى هذا القانون، والتي سمحت لقاضي التحقيق أن يصدر

(72) د.حسن الجوخدار: المرجع السابق، الجزء الثاني، ص 158.

(73) المستشار الدكتور عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص389. د.سليمان أحمد فضل: المرجع السابق، ص307.

(74) نبيلة هبة هروال: المرجع السابق، ص 226.

(75) القاضي الدكتور غسان رباح: المرجع السابق، ص 159.

إذن بتفتيش نظم المعلومات[76].

وفي سورية فقد اعتبرت الفقرة (ب) من المادة 26 من قانون مكافحة الجريمة المعلوماتية البرمجيات الحاسوبية من الأشياء المادية التي يجوز تفتيشها وضبطها، وفق القواعد المنصوص عليها في قانون أصول المحاكمات الجزائية.

ومن الأمثلة الواقعية لتفتيش برامج الحاسوب، أنه بعد تفجير بُرجي مركز التجارة العالمي في الولايات المتحدة الأمريكية في2001/9/11، ولدى تفتيش الحاسوب النقال العائد للمشتبه به "رمزي يوسف" تبيّن – بحسب رأي الـ FBI– بأن هذا الحاسوب كان يحوي الخطط اللازمة للقيام بعمليتي التفجير، كما أدّى هذا التفتيش إلى الكشف عن دور المدعو "زكريا الموسوي" في عملية التفجير الثانية. وقد تمّ فحص وتفتيش أكثر من مئة قرص صلب في هذه التحقيقات[77].

وفي قضية أخرى، تتلخص وقائعها بأن السيدة "شارون لوباتكا" غادرت منزلها بقصد زيارة صديقتها، إلا أنها تغيبت عن المنزل لعدة أيام، ولدى تفتيش الحاسوب الشخصي العائد لها، وجدت الشرطة مئات الرسائل الإلكترونية بين السيدة "شارون" وشخص يدعى "روبرت غلاس"، وقد تضمنت هذه الرسائل تخيلات عن التعذيب والموت. ولدى قيام الشرطة بالتحقيق مع "غلاس"، اعترف بأنه قتل شارون خطأً أثناء نومه معها، كما قام بإرشاد الشرطة إلى مكان جثتها في شمال كاليفورنيا، حيث وجدت الشرطة أيدي وأرجل شارون مربوطة، ثم تبين أنها ماتت خنقاً[78].

2–تفتيش شبكات الحاسوب:

من المشكلات التي تواجه القائم بالتفتيش، مشكلة اتصال الحاسوب موضوع التفتيش بحاسوب آخر موجود داخل أو خارج إقليم الدولة. فكثيراً ما يقوم مرتكب الجريمة بتخزين معلوماته في حواسيب أو مُخدّمات أخرى؛ بهدف عرقلة التحقيقات. والسؤال الذي يطرح نفسه هنا هو:

هل يشمل التفتيش الحواسيب الأخرى المرتبطة بالحاسوب المطلوب تفتيشه؟

للإجابة على هذا السؤال هناك احتمالان:

(76) د. عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق، ص 854.

(77) Eoghan Casey, op-cit, p-19.

(78) Eoghan Casey, op-cit, p-20.

الاحتمال الأول: أن يكون حاسوب المتهم متصلاً بحاسوب أو مُخدّم موجود في مكان آخر داخل الدولة.

هناك من يرى في **الفقه الألماني** أنه في هذه الحالة يمكن أن يمتد التفتيش إلى المعلومات والبيانات المخزنة في حاسوب أو مُخدّم الآخر، وذلك استناداً إلى القسم 103 من قانون الإجراءات الجزائية الألماني.

وفي **هولندا** نصت المادة 125 من مشروع قانون الحاسوب على جواز أن يمتد التفتيش في هذه الحالة إلى نظم المعلومات الموجودة في حاسوب أو مُخدّم آخر، بشرط أن تكون هذه المعلومات والبيانات ضرورية لإظهار الحقيقة، وذلك مع مراعاة بعض القيود[79].

أما الفقرة الثانية من المادة 19 من **الاتفاقية الأوربية حول الجريمة الافتراضية لعام 2001**، فقد سمحت بتفتيش نظام حاسوب آخر أو جزء منه، إذا كان هناك أساس يدعو إلى الاعتقاد بأن البيانات المطلوبة قد تمّ تخزينها في نظام ذاك الحاسوب، بشرط أن يكون نظام الحاسوب الآخر ضمن النطاق الإقليمي للدولة[80].

الاحتمال الثاني: أن يكون حاسوب المتهم متصلاً بحاسوب أو مُخدّم آخر موجود في مكان آخر خارج الدولة.

في هذه الحالة هناك من يرى في **الفقه الألماني** أن استرجاع المعلومات والبيانات التي تم تخزينها في الخارج يعتبر انتهاكاً لسيادة الدولة الأخرى[81].

أما المادة 125 من مشروع قانون الحاسوب **في هولندا**، فقد سمحت بتفتيش نظم الحاسوب

---

(79) Kaspersen (W.K.Henrik):"computer crime and crime against information in Netherlands"R.I.D.p1993,p.479.
مشار إليه عند المستشار الدكتور عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرام الكمبيوتر والإنترنت، المرجع السابق، ص 381 – 382. د.علي الطوالبة:المرجع السابق،ص40–41. نبيلة هبة هروال: المرجع السابق، ص 239–240.

(80) المادة /19/ من الاتفاقية الأوربية. د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية،المرجع السابق، ص 149 وما بعدها.

(81) Mohrenschl ager (Manfred):computer crimes and other crimes against information technology in GermanyR.I.P,1993, p.351.
مشار إليه عند المستشار الدكتور عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرام الكمبيوتر والإنترنت، المرجع السابق، ص 382.

المرتبطة بحاسوب المتهم، حتى ولو كانت موجودة في دولة أخرى، بشرط أن يكون هذا التدخل مؤقتاً، وأن تكون المعلومات والبيانات لازمة لإظهار الحقيقة(82).

أما المادة 32 من **الاتفاقية الأوربية حول الجريمة الافتراضية لعام 2001**، فقد سمحت بتفتيش حاسوب موجود في دولة أخرى في حالتين: الأولى إذا تعلق التفتيش ببيانات متاحة للجمهور. والثانية إذا رضي صاحب البيانات بالتفتيش(83).

وقد حسم المشرع السوري هذا الخلاف بالفقرة (ج) من المادة 26 من قانون مكافحة الجريمة المعلوماتية، التي أجازت تفتيش الأجهزة والبرمجيات الحاسوبية **المتصلة بأجهزة المشتبه فيه**، أيّاً كان مكان وجودها، ضمن حدود الواقعة المسندة إلى المشتبه فيه. أي سواء أكانت هذه الأجهزة موجودة داخل سورية أم خارجها، بشرط أن يكون التفتيش في حدود ضرورات كشف الواقعة الجرمية.

ففي إحدى قضايا الاحتيال عبر الإنترنت، تبين بنتيجة البحث أن حاسوب المتهم الموجود في ألمانيا متصل بحواسيب أخرى في سويسرا، حيث تم تخزين المعلومات في هذه الحواسيب الخارجية. وعندما رغبت السلطات الألمانية بالحصول على هذه المعلومات، لم تستطع ذلك إلاّ من خلال طلب المساعدة المتبادلة(84).

وفي اليابان، قامت مجموعة من المخربين بمهاجمة العديد من المواقع الخاصة في الحكومة اليابانية، واستخدموا في ذلك حواسيب موجودة في الصين والولايات المتحدة الأمريكية. وقد طلبت الشرطة اليابانية المساعدة من بكين وواشنطن من أجل تسليم المعلومات والبيانات المسجلة على هذه الحواسيب في كلتا الدولتين، حتى تتمكن من التوصل إلى هؤلاء المجرمين(85).

ومن الجدير بالذكر أن الفقرة (د) من المادة 26 من قانون مكافحة الجريمة المعلوماتية ألزمت

---

(82) Durham (colo):The emerging structures of criminal information law: tracing the contours of a new pardign general report for the A.I.D.P. 1993,p.115.

مشار إليه عند المستشار الدكتور عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 383.

(83) المادة /32/ من الاتفاقية الأوربية. د.عمر بن يونس: الاتفاقية الأوربية حول الجريمة الافتراضية،المرجع السابق، ص227.

(84) المستشار الدكتور عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 383.

(85) المستشار الدكتور عبد الفتاح بيومي حجازي: مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 383.

مقدّمي الخدمة على الشبكة الالتزام بالحفاظ على **سرية الإجراءات** التي تقوم بها الضابطة العدلية المختصّة في جميع الحالات. كما ألزمت الفقرة (هـ) من هذه المادة كل صاحب أو مدير أي منظومة معلوماتية تُرتكب جريمة معلوماتية باستخدام منظومته، أن **يتيح للضابطة العدلية** تفتيش وضبط البيانات والمعلومات والبرمجيات الحاسوبية، والحصول على نسخة منها؛ ويمكن للضابطة العدلية في حالات الضرورة ضبط الأجهزة والبرمجيات الحاسوبية المستخدمة أو جزء من مكوّناتها. وقد **عاقب** المشرع في الفقرة (و) على مخالفة أحكام المادة 26 بالحبس من شهر إلى ستة أشهر والغرامة من مئة ألف إلى خمسمئة ألف ليرة سورية.

خامساً– الضبط:

الضبط هو الأثر المباشر للتفتيش. فالعلاقة وثيقة بين التفتيش والضبط، فإذا بطلت إجراءات التفتيش بطل الضبط. وقد يتم الضبط من غير تفتيش، عندما يقدم المشتبه به باختياره الأشياء المتعلقة بالجريمة [86].

والضبط هو الوسيلة القانونية التي تضع بواسطتها السلطة المختصة يدها على جميع الأشياء التي وقعت عليها الجريمة أو نتجت عنها أو استعملت باقترافها، كالأسلحة والأشياء المسروقة، والثياب الملوثة بالدم، والأوراق... وغير ذلك[87].

وقد أجاز القانون السوري ضبط كل ما يعدّ من آثار الجريمة، وسائر الأشياء والأوراق التي تساعد على إظهار الحقيقة، سواء أكانت تؤيد التهمة أم تنفيها. وقد أوجب القانون عرض الأشياء المضبوطة على المدعى عليه أو على من ينوب عنه للمصادقة والتوقيع عليها، فإذا امتنع، صرّح القائم بالضبط بذلك في المحضر[88].

أما بالنسبة إلى **إجراءات ضبط المكونات المعنوية للحاسوب والإنترنت**، فإن البيانات والمعلومات لا يمكن ضبطها بشكل منفصل عن أجهزة وأدوات التخزين، فالحاسوب والأجهزة الملحقة به، هي بمثابة الأوعية المادية التي تحتوي هذه المعلومات والبيانات، وهي تشبه الحقيبة التي تُحفظ فيها الأوراق. وقد أجاز المشرع في الفقرة (هـ) من المادة 26 من قانون مكافحة الجريمة المعلوماتية للضابطة العدلية

(86) د.علي الطوالبة: المرجع السابق، ص127.

(87) د.حسن الجوخدار: المرجع السابق، الجزء الثاني، ص 162.

(88) المواد 32، 34، 97 من قانون أصول المحاكمات الجزائية.

الحصول على **نسخة** من البيانات والمعلومات والبرمجيات الحاسوبية التي تم تفتيشها؛ **ويمكن للضابطة العدلية في حالات الضرورة ضبط الأجهزة** والبرمجيات الحاسوبية المستخدمة أو جزء من مكوّناتها.

ولذلك يرى الفقه المقارن أن على رجل الضابطة العدلية عندما يصل إلى مسرح الجريمة، أن يتبع في ضبط المعلومات الرقمية الإجراءات التالية(89):

- تأمين مسرح الجريمة الرقمية من العبث، إذ يجب عزل الحواسيب عن الشبكة، لتجنب إجراء أي تغيير على الأدلة الرقمية من قبل الغير. كما يجب رفع البصمات عن الأجهزة لمقارنتها فيما بعد ببصمة المشتبه به.
- حجز الحاسوب أو القرص الصلب، وجميع الحاويات المادية والذواكر، كالسواقات والأقراص الممغنطة.
- وضع ملصقات على الأشياء المضبوطة، وتوثيقها وتغليفها، وتحضيرها لنقلها بالحالة التي كانت عليها إلى مكان الاختبار والفحص.
- تحرير محضر بعد إجراء عملية الفحص، يتضمن ذكر جميع الإجراءات السابقة، والنتائج التي تم التوصل إليها بنتيجة الفحص.

وبناءً على ذلك، فإن ضبط الأدلة الرقمية يجب أن يتناسب مع ماهيتها، بحيث ينصبّ الضبط على جميع الأجهزة والأدوات التي تمّ تخزين المعلومات فيها، لأن ضبط المعلومات والبيانات لا يمكن أن يتم بمعزل عن وسائط التخزين.

---

(89) Anthony Reys and others, op-cit, P-141-142 .

تمارين:

اختر الإجابة الصحيحة: في سورية:

1- لم يحدد ينص المشرع السوري في قانون مكافحة الجريمة المعلوماتية على ضابطة خاصة لمكافحة جرائم المعلوماتية.
2- نص المشرع السوري في قانون مكافحة الجريمة المعلوماتية على إحداث ضابطة خاصة لمكافحة جرائم المعلوماتية.
3- نص المشرع السوري في قانون مكافحة الجريمة المعلوماتية على إحداث مكتب خاص في وزارة العدل لمكافحة جرائم المعلوماتية.
4- جميع الإجابات السابقة خاطئة.

الإجابة الصحيحة رقم 2

الأحكام الإجرائية للجريمة المعلوماتية

الوحدة التعليمية السادسة

3- طرق الإثبات المستحدثة (الدليل الرقمي)

الكلمات المفتاحية:

ماهية الدليل الرقمي- تعريف الدليل الرقمي-مزايا الدليل الرقمي - مساوئ الدليل الرقمي - مصادر الدليل الرقمي- حجية الدليل الرقمي.

الملخص:

تتضمن هذه الوحدة التعليمية تعريف الدليل الرقمي ومزايله ومساوئه ومصادره ، وشروط حجية هذا الدليل أمام القضاء في بعض الدول الآخرى وفي سورية.

الاهداف التعليمية:

في نهاية هذه الوحدة التعليمية يجب أن يكون الطالب قادراً على تمييز مفهوم الدليل الرقمي ومزايله ومساوئه ومصادره، وشروط حجية هذا الدليل أمام القضاء في سورية، مع ضرب الأمثلة العملية عليه.

لم تَسلَم طرق الإثبات من تأثيرات ثورة المعلومات والتكنولوجيا، فالتناغم المطلوب تحقيقه دائماً بين طبيعة الدليل وطبيعة الجريمة التي يولد منها، أفرز إلى حيز الوجود نوعاً جديداً من الأدلة يتماشى مع طبيعة جرائم المعلوماتية، وهو ما يعرف بالدليل الرقمي، أي الدليل الناتج عن فحص المكونات المعنوية أو البرمجية للحواسيب وشبكة الإنترنت.

فإذا كان فحص السلاح الناري والذخيرة هو المولد للدليل في جريمة القتل، وفحص المحرر هو المولد للدليل في جريمة التزوير؛ فإن جرائم المعلوماتية لا تخرج عن هذا الإطار، فإثبات هذه الجرائم يحتاج إلى طرق تقنية تتناسب مع طبيعتها، بحيث يمكن ترجمة النبضات والذبذبات الإلكترونية إلى أدلة إثبات أو نفي على ارتكاب هذه الجرائم.

وقد ساهم القضاء المقارن في رسم معالم الدليل الرقمي، سواء من حيث فائدته أم من حيث قيمته القانونية، حيث اعتّدت به المحاكم بناء على نص تشريعي تارة، وعلى الاجتهاد تارة أخرى.

ماهية الدليل الرقمي

يتطلب منا البحث في ماهية الدليل الرقمي التعرض لتعريفه، ثم التعرف على مزايا ومساوئ هذا الدليل، وتحديد مصادره الرقمية، وبيان الدور الذي يلعبه الدليل الرقمي في التحقيقات الجرمية، وهذا ما سنبحثه على التتالي:

أولاً- تعريف الدليل الرقمي:

عرف المشرع **الدليل الرقمي** في المادة الأولى من قانون مكافحة الجريمة المعلوماتية بأنه : (البيانات الرقمية المخزّنة في الأجهزة الحاسوبية أو المنظومات المعلوماتية، أو المنقولة بواسطتها، والتي يمكن استخدامها في إثبات أو نفي جريمة معلوماتية).

و من خلال استقراء هذا التعريف، يمكن تحديد خاصتين للدليل الرقمي هما:

الخاصة الأولى: إن الدليل الرقمي عبارة عن معلومات أو بيانات رقمية مخزنة في الحاسوب أو منقولة بواسطته، أيّاً كان شكل هذا الحاسوب، بحيث يستوي أن يتخذ شكل الحاسوب الشخصي، أو مُخدّم الإنترنت، أو أن يكون ضمن الهاتف الجوال، أو ساعة اليد، أو الكاميرات الرقمية وغيرها.

الخاصة الثانية: القيمة الاستدلالية أو البرهانية لهذه المعلومات في إثبات أو نفي الجرائم.

ثانياً- مزايا الدليل الرقمي:

يتمتع الدليل الرقمي بعدة مزايا، وهي:

أ-إمكانية النسخ:

يمكن نسخ الدليل الرقمي نسخة مطابقة للأصل تماماً، بحيث يمكن إجراء الفحص المعلوماتي على هذه النسخة لتفادي خطر إتلاف النسخة الأصلية أثناء عملية الفحص، وهذه الميزة لا تتوفر في الأدلة التقليدية[1].

ب-إمكانية كشف التعديل:

قد يتعرض الدليل الرقمي للتعديل المقصود من قبل الجاني، أو التعديل غير المقصود من قبل المحقق أو الخبير المعلوماتي أثناء عملية جمع الدليل، وفي كلتا الحالتين يمكن معرفة ما إذا كان الدليل الرقمي قد تعرض للتعديل أم لا، وذلك باستخدام برمجيات تقنية معينة تستخدم في هذا الخصوص، إضافةً إلى إمكانية إجراء المقارنة مع النسخة الأصلية إن وجدت[2].

---

(1). Eoghan Casey: op-cit, P-25

(2). Eoghan Casey: op-cit, P-25

جـ- صعوبة التخلص من الدليل الرقمي:

و هذه الميزة من أهم مزايا الدليل الرقمي على الإطلاق، بل يمكن القول بأنها الميزة التي يتمتع بها الدليل الرقمي دون غيره من الأدلة التقليدية، وهو بذلك يشبه الدليل العلمي المتعلق بالحمض النووي DNA، إذ إن كليهما يصعب التخلص منهما.

ففي مجال الأدلة التقليدية، كثيراً ما كانت أجهزة العدالة تعاني من مسألة التخلص من الأدلة المادية، إذ يمكن التخلص من بصمات الأصابع بمسحها من موضعها، ويمكن التخلص من الأوراق التي تحمل إقرارات معينة بتمزقها وحرقها، كما يمكن التخلص من الشهود بقتلهم أو تهديدهم بهدف عدم الإدلاء بشهاداتهم. وفي جميع هذه الحالات يكون من الصعب إن لم يكن مستحيلاً استرجاع أو استرداد هذه الأدلة.

أما في حالة الدليل الرقمي فالأمر يختلف تماماً. فمسألة التخلص من الملفات الإلكترونية عن طريق تعليمات Delete أو Erase أو حتى في حالة إعادة تهيئة القرص الصلب Format وغيرها، لا تشكّل عائقاً يحول دون استرجاع هذه الملفات-كلياً أو جزئياً- التي تمّ إلغاؤها أو إزالتها من الحاسوب(3).

ومن القضايا التي أبرزت هذه الميزة، أنه أثناء التحقيق مع الكولونيل "أوليفر نورد" في قضية إيران عام 1986، تمّ استعادة جميع الرسائل الإلكترونية المتعلقة بالجريمة، بعد أن قام هذا الكولونيل بحذفها من حاسوبه، إذ لم يكن هذا الأخير يعلم بأن هذه الرسائل يمكن استعادتها عن طريق النسخ المحفوظة في النظام(4).

ثالثاً- مساوئ الدليل الرقمي:

للدليل الرقمي عدة مساوئ، وهي:

أ-الدليل الرقمي دليل غير مرئي:

ليس للدليل الرقمي طبيعة مادية ملموسة كما هو الحال في الأدلة التقليدية، فالأجهزة التقنية لا تفرز سكيناً عليها بصمات القاتل، أو مالاً يمكن ضبطه مع السارق في جريمة السرقة وغير ذلك، فكل ما تنتجه التقنية هو عبارة عن نبضات إلكترونية يمكن أن تدل في مجموعها على أنماط السلوك الإنساني.

و الواقع أن هذه الطبيعة غير المرئية للدليل الرقمي تلقي بظلالها على أجهزة الضبط القضائي

---

(3) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق، ص 981، 982، 983.

Eoghan Casey: op-cit, P-26 .(4)

التي تتعامل مع هذه الجرائم المستحدثة، لأن غياب الدليل المرئي يشكّل عقبة كبيرة أمام كشفها[5].

ب-الحجم الكبير للبيانات التي يوجد فيها الدليل الرقمي:

يحتوي القرص الصلب مثلاً على حجم كبير من البيانات والمعلومات غير المرتبة، ولكن ما يتعلق بالجريمة قد يشكل جزأً صغيراً فقط من هذه المعلومات. و يمكن تشبيه حجم المعلومات هذا بموجات الراديو الموجودة في الهواء والتي تحتوي على بيانات متشابكة، الأمر الذي يجعل من الصعوبة بمكان معرفة الإشارة المطلوبة وترجمتها إلى بيانات مفهومة. فالوصول إلى الدليل الرقمي المطلوب يشكّل تحدياً أمام الخبير المعلوماتي[6].

جـ- الدليل الرقمي دليل ظرفي:

الدليل الرقمي هو عادة دليل ظرفي، فمعرفة عنوان الإنترنت IP مثلاً يشير إلى الحاسوب الذي ارتكبت الجريمة بواسطته فقط، دون أن يحدّد مرتكب الجريمة بالذات، الأمر الذي يجعل من الصعوبة بمكان، نسبة النشاط الجرمي إلى شخص ما، ما لم يتم القيام بالعديد من التحقيقات للتأكد من ذلك.

ففي إحدى القضايا التي عرضت على المحاكم الأمريكية، نازع المدعى عليه في جميع الأدلة التي وجدت على حاسوبه، لأن المحققين لم يستطيعوا إثبات أنه هو الشخص الذي قام بالنشاطات غير الشرعية على الإنترنت[7].

وتجدر الملاحظة في هذا المجال إلى أن المساوئ المشار إليها، والتي تقف في وجه الدليل الرقمي في هذه الأيام، قد لا يكون لها أثر في القريب العاجل، لأن التطور المتسارع للبرمجيات في عصر الثورة الرقمية قادر على إزالة معظم الصعوبات التي تقف حائلاً دون نمو هذا الدليل المستحدث.

رابعاً- مصادر الدليل الرقمي ودور الإنترنت في التحقيقات الجرمية:

يمكن الوصول إلى الدليل الرقمي المتعلق بجرائم المعلوماتية عن طريق البحث في المصدرين التاليين:

أ-أنظمة الحاسوب وملحقاتها:

تعدّ الحواسيب مصدراً غنياً بالأدلة الرقمية، وخاصة تلك الحواسيب الشخصية التي تعدّ بمثابة أرشفة سلوكية للأفراد. فهذه الحواسيب تحتوي على الكثير من المعلومات المتعلقة بنشاطات الأفراد ورغباتهم.

---

(5) د.جميل عبد الباقي الصغير: الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، المرجع السابق، ص4. د.علي محمود علي حمودة: المرجع السابق، ص16. متوفر على الموقع www.arblawinfo.com.

(6). Eoghan Casey: op-cit, P-25

(7). Eoghan Casey: op-cit, P-26

فالملفات الشخصية أو ملفات النظام وغيرها من أنواع الملفات، التي تكون مخزنة عادة في الأقراص الصلبة أو الأقراص الليزرية CD أو الذواكر المعروفة بـ Flash Memory[8] كثيراً ما تحتوي على معلومات تتعلق بالجريمة وتفيد في عملية التحقيق[9].

وعملية حجز الحاسوب أو ضبطه بقصد تفحصه، تعدّ نقطة البداية في الكشف عن خفايا جريمة المعلوماتية، لأن الحاسوب هو وسيلة النفاذ إلى هذه الشبكة، أيّاً كان شكل هذا الحاسوب. ويجب أن تشمل عملية الفحص جميع البرمجيات المخزنة في المكونات الصلبة أو الذواكر الملحقة بالحاسوب، وجميع البرمجيات التي تمّ إلغاؤها من ذي قبل، كما يجب التأكد من أن المكونات الصلبة والبرمجيات تعمل بشكل سليم ومنتظم، وأن الحاسوب غير مصاب بفيروس يؤثر على نظامه أو على ملفات التشغيل أو التنفيذ، لأن ذلك يمكن أن ينال من صحة الدليل الرقمي المستخلص عند عرضه على القضاء[10].

ب-أنظمة الاتصال بالإنترنت:

تشمل عملية فحص أنظمة الاتصال بالإنترنت، فحص حركة التنزيل والتحميل ودرجة الاستيعاب، والشبكات المحلية، والنظام الأمني المحاط بالإنترنت...الخ. فعملية الفحص هذه قد تؤدي إلى الحصول على دليل رقمي يفيد في كشف الحقيقة[11].

ولعلّ أهم المسائل المثارة في صدد فحص أنظمة الاتصال بالإنترنت هي مسألة تحديد مكان الجريمة، أو الحاسوب الذي ارتكب بواسطته النشاط الجرمي، حيث يمكن معرفة هذا الحاسوب عن طريق تتبع الحركة العكسية لمسار الإنترنت[12]، ويستخدم في عملية التتبع هذه نظام فحص إلكتروني يطلق عليه **علم البصمات المعاصر أو علم بصمات القرن الواحد والعشرين**، وهو منهج تم استخدامه في العديد من الجرائم، مثل تتبع مبتكر فيروس "ميليسا"، وكذلك في التوصل إلى الشخص الذي ابتكر موقع خدمات "بلومبرمج" لأخبار المال، وهو موقع احتيالي يرفع أسعار الأسهم بطريقة الخداع.[13]

---

(8) ذاكرة سريعة بحجم القلم، ذات سعة كبيرة ومحمولة، يمكن ربطها بالحاسوب الشخصي وتسجيل ملفات ذات حجم كبير. د.عبد الحسن الحسيني: المرجع السابق، ص526.

(9) Eoghan Casey : op-cit, p-21. And also Albert . J. Marcella, cyber forensics, field manual for collecting Examining and preserving Evidence of computer crimes , published by CRC press , 2002 p94-95 and also Robin Bryant, op-cit,p-50.

(10) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق، ص 1008- 1009.

(11) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق، ص 333- 997.

(12) يقصد **بمسار الإنترنت**، الحركة التراسلية للنشاط الممارس من خلال الإنترنت، فالحاسوب بمجرد أن يتعرف على المسار، يقوم تلقائياً باختيار البروتوكول التراسلي الذي من خلاله يقوم باستدعاء البيانات، وهذه هي الحركة التي أشار إليها علماء الإنترنت بأنها تتشابه مع شبكة العنكبوت من حيث عدم انتظام شكل المسار الاتصالي والتواصلي عبرها. د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق، ص 998.

(13) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق، ص 998.

ومن الملاحظ أن ما يتم التوصل إليه بفضل تتبع الحركة العكسية لمسار الإنترنت هو عنوان رقمي فقط IP adress، وهذا الدليل الرقمي لا يكفي لنسبة الجريمة إلى مالك الحاسوب، إذ من الممكن ألاّ يكون هو مرتكب الجريمة، كما لو كان حاسوبه مسروقاً، أو مؤجراً في أحد مقاهي الإنترنت، أو أن يكون عنوانه الرقمي الخاص به مسروقاً، أو أن يكون هناك من يستخدم حاسوبه دون تصريح من مالكه، أو أن المشتبه به لا يعرف أي شيء عن الإنترنت...الخ. الأمر الذي يتطلب من جهات التحقيق توفير الدليل المادي كالاعتراف أو الشهادة أو الخبرة...الخ إلى جانب الدليل الرقمي، حتى يمكن أن تنسب الجريمة إلى مرتكبها[14].

أما مُخدّمات شبكة الإنترنت، فهي تحتوي على الكثير من المعلومات حول أنماط سلوك الأفراد في وقت محدد، فيمكن عن طريق فحص هذه المُخدّمات معرفة الرسائل الإلكترونية التي قام الجاني أو المجني عليه بإرسالها أو استقبالها، والمواقع الإلكترونية التي سبقت زيارتها، وغرف الدردشة التي تمّ الدخول إليها، حيث يستطيع المحقق أو الخبير المعلوماتي بعد أن يصل إلى هذه المعلومات، أن يتصل بجميع الأفراد الذين كانوا على اتصال مع الجاني أو المجني عليه قبل ارتكاب الجريمة، وذلك عن طريق إرسال الرسائل الإلكترونية إليهم، وسؤالهم عن أي معلومات تتعلق بالجريمة[15].

وعلى المحقق أو الخبير المعلوماتي أن يوثق جميع مراحل عملية البحث، بحيث يشير إلى زمان البحث ومكان المعلومة وكيفية الحصول عليها، وأن يستخدم البرمجيات التي تحافظ على مواقع الوبّ التي عمل بها؛ لأنه من المعروف أن المعلومات تتغير على الإنترنت من لحظة إلى أخرى[16].

وقد يتخذ الدليل الرقمي المستمد من الحاسوب أو الإنترنت شكل المخرجات الورقية التي يتم الحصول عليها عن طريق الطابعات أو الراسمات، كما يمكن أن يتخذ الشكل الإلكتروني كالأقراص الليزرية وغيرها من الأشكال الإلكترونية. وإلى جانب ذلك يوجد مخْرَج ثالث وهو عرض المعلومات والبيانات المتعلقة بالدليل الرقمي عن طريق شاشة الحاسوب. ويطلق على جميع هذه الأشكال مصطلح **مخرجات الحاسوب**[17].

ومن أمثلة القضايا التي تظهر دور الإنترنت في عملية التحقيق، قضية تتعلق بالاحتيال عبر الإنترنت، تتلخص وقائعها بقيام شخص يدعى "كوري ستيل" Cory Steele من ولاية "مينسوتا" الأمريكية، وهو صاحب شركة لتجارة الأدوية اسمها Advanced Express System، بإنشاء موقع

---

(14) د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق، ص 999.

(15) Eoghan Casey: op-cit, P-451.

(16) Eoghan Casey: op-cit, P-452.

(17) د.هلالي عبد اللاه أحمد: حجية المخرجات الكمبيوترية في المواد الجنائية، النسر الذهبي للطباعة– القاهرة، 2002، ص15–16.

لصيدلية غير شرعية على الإنترنت باسم Swift RX.com، حيث كان يقوم بالاحتيال على الناس عبر هذا الموقع، عن طريق عرض الأدوية للبيع بدون وصفات طبية، وتلقي الثمن عبر الإنترنت من خلال بطاقات الائتمان، وعدم إرسال هذه الأدوية إلى المشترين.

وقد بدأت مجريات هذه القضية عندما لاحظ أحد المستأجرين في البناء الذي يوجد فيه مقر شركة المدعو "كوري" مظاهر الثراء الفاحش على هذا الأخير، الذي كان يملك عدة سيارات فخمة مثل Lamborghini، Ferrari،Mercedes، فقام هذا الجار بالبحث عن اسم الشركة عبر الإنترنت، حيث تبين له أن لهذه الشركة عدة مواقع إلكترونية، وأن هناك الكثير من الأشخاص الذين كانوا يشتكون من احتيالات هذه الشركة. عندها اتصل بمكتب التحقيقات الفيدرالي FBI وأعلمهم بهذه المعلومات.

وبعد تلقي هذا الإخبار، بدأ أحد المحققين في مكتب التحقيقات الفيدرالي بجمع معلومات إضافية عن المدعو"كوري" وذلك عن طريق محركات البحث مثل googleو whois، حيث تبين بأن الموقع الإلكتروني للصيدلية Swift RX.com كان مسجلاً على مزود خدمة إنترنت في سويسرا، وله عنوان تجاري في المملكة المتحدة، وكان ذلك بهدف عرقلة عملية التعقب من قبل المحققين، كما تبين بأن هناك العديد من مواقع الصيدليات غير الشرعية على الإنترنت التي تعود لشركة المدعو "كوري"، وهذه المواقع مسجلة تحت أسماء وعناوين مختلفة في الولايات المتحدة الأمريكية، ومستضافة من قبل مزودي خدمة الإنترنت في تكساس، وأوهايو، ومينيسوتا.

كما توصل المحقق المسؤول عن هذه القضية إلى معلومات تفيد بأن المدعو "كوري" كان يستخدم مبرمجة حاسوب لاختراق المواقع الإلكترونية للصيدليات المنافسة عبر الإنترنت، وذلك بهدف سرقة المعلومات المتعلقة بالزبائن، إضافةً إلى أن "كوري" كان يتعامل مع مجموعة من الأفراد القادرين على سرقة عناوين الإنترنت، حيث كانت هذه العناوين المسروقة تستخدم في إرسال الإعلانات الدوائية الوهمية إلى الزبائن.

وبعد جمع هذه المعلومات من قبل المحقق، قام بإرسال تقريره إلى معاونة المحامي العام في أمريكا، التي قامت بتشكيل فريق لمتابعة التحقيق والبحث عن معلومات إضافية تتعلق بالمدعو "كوري"، وقررت على الفور إغلاق مواقع الصيدليات غير الشرعية على الإنترنت، وأصدرت عدة مذكرات تفتيش لمقر الشركة، حيث قام فريق التحقيق بمصادرة مجموعة من الحواسيب من هذا المقر.

وقد تمّ مراجعة وتدقيق جميع الأدلة الحاسوبية والوثائقية، كما تمّ ضبط جميع الرسائل الإلكترونية بين المشتبه به وشركائه، حيث أعطت هذه الرسائل الصورة الحقيقية لأعمال المدعو "كوري" والتاريخ الكامل لهذه الأعمال، كما تمّ سماع ما يقرب من مئة شاهد في هذه القضية. وقد تبيّن بأن مبيعات الصيدليات غير الشرعية كانت تصل إلى /28/ مليون دولار شهرياً من خلال استخدام/17/

موقعاً إلكترونياً.

أما المدعو "كوري"، فقد تمّ إلقاء القبض عليه في المطار بعد عودته من الخارج، حيث كان يقوم بالبحث عن أماكن ليؤسس فيها أعماله في الخارج، وقد حُكم عليه بالسجن لمدة /20/ عاماً، وبمصادرة ما يعادل خمسة ملايين دولار من ممتلكاته[18].

ومن الملاحظ بأن الدليل الرقمي يتمتع بأهمية بالغة في عملية التحقيق بجرائم المعلوماتية، إلاّ أنه لا بدّ من أن يكون هناك دائماً أدلة مادية (كالاعتراف أو الخبرة الفنية مثلاً) يتم الاستناد إليها إلى جانب الدليل الرقمي حتى تكتمل صورة الجريمة.

---

(18) Joseph T. wells: Computer fraud casebook, published by john wiely@sons.inc, Hoboken, New Jersey, 2009, p1-10.

حجية الدليل الرقمي

لا تقف الصعوبات التي تواجه الدليل الرقمي عند حد كيفية الحصول عليه وإجراءات حفظه، بل تمتد إلى مدى القوة الثبوتية التي يتمتع بها هذا الدليل، ومدى حرية قاضي الموضوع بالاقتناع به لبناء الحكم على أساسه بالبراءة أو الإدانة. لذلك حاول المشرع والقضاء والفقه المقارن التصدي لهذه المسألة، وذلك بتحديد الشروط التي يجب توفرها في الدليل الرقمي أو في مخرجات الحاسوب حتى يمكن قبوله من قبل القاضي الجزائي.

وبناء على ما تقدم، سنتناول حجية الدليل الرقمي في الولايات المتحدة الأمريكية وإنكلترا وفرنسا، والمنظمة الدولية لدليل الحاسوب.

أولاً- الولايات المتحدة الأمريكية:

تبنّى قانون الإثبات الفيدرالي في المادة /1002/ منه قاعدة **الدليل الأفضل**، ويقصد بهذه القاعدة أنه عند إثبات مضمون كتابات أو سجلات أو صور، فإن أصل هذه الكتابات أو السجلات أو الصور يجب أن يكون متوفراً، أي يجب تقديمه إلى المحكمة[19].

وقاعدة الدليل الأفضل التي تعبر عن أصالة الدليل تقف حائلاً أمام الدليل الرقمي، لأن ما يتم تقديمه إلى المحكمة ليس الملفات الإلكترونية المخزنة في الحاسوب، وإنما نسخ عن هذه الملفات. ولذلك فقد حسم المشرع الأمريكي هذه المسألة لصالح الدليل الرقمي في المادة 1001/3 من قانون الإثبات الأمريكي والتي نصت على ما يلي:

(إذا كانت البيانات مخزنة في حاسوب أو آلة مشابهة، فإن أي مخرجات مطبوعة منها أو مخرجات يمكن قراءتها بالنظر إليها وتعكس دقّة البيانات، تعدّ بيانات أصلية) [20].

---

(19) The Federal Rules of Evidence.

يتضمن هذا القانون القواعد المقبولة في الإثبات أمام المحاكم الاتحادية في الولايات المتحدة الأمريكية، في حين أن محاكم الولايات تتبع قواعدها الخاصة مثل "كاليفورنيا" و"واشنطن". وقدُ وِضعَ هذا القانون بناء على اقتراح المحكمة العليا في الولايات المتحدة الأمريكية أول مرة عام 1975، وجرى تعديله عدة مرات، وهو متوفر على الإنترنت مع تعديلاته حتى 2008/12/1 على الموقع www.wikipedia.org أو www.lawsource.com ومشار إليه عند د.عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق، ص988.

(20) Albert .J. Mercella, op-cit, 26.

وأيضاً د.عمر بن يونس: الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي،المرجع السابق، ص 441.

ووفقا لهذه المادة، فإن البيانات أو المعلومات التي تمّ الحصول عليها من الإنترنت، والتي تمّ استخراجها بواسطة الطابعة، تعدّ دليلاً أصلياً كاملاً، ولا حاجة لجلب الحاسوب إلى قاعة المحكمة.

أما فيما يخص القوة الإثباتية للسجلات الإلكترونية، فإن المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب الصادر في عام 2002 يميز بين نوعين من السجلات، وهما:

النوع الأول- السجلات المخزنة في الحاسوب:

وهي الوثائق الإلكترونية التي تحتوي على كتابات عائدة لشخص ما، ومن أمثلتها رسائل البريد الإلكتروني، وملفات الورد Word، ورسائل غرف الدردشة على الإنترنت. وهذه الوثائق تتضمن إفادات بشرية، وتعدّ كالشهادة على السماع في مجال الإثبات(21).

النوع الثاني- السجلات المأخوذة من الحاسوب:

وهي عبارة عن نتائج برامج الحاسوب التي لا تمسها الأيدي البشرية، ومن أمثلتها سجلات الدخول إلى الإنترنت، وسجلات الهاتف، وإيصالات الصراف الآلي وغيرها. فهذه السجلات لا تتضمن إفادات بشرية، وإنما هي عبارة عن نتائج البرامج الحاسوبية. فالصراف الآلي مثلاً يمكن أن يعطي إيصالاً يتضمن أن /100/ دولار أمريكي قد تم إيداعها في الحساب عند الساعة 2.25 مساءً، وهذا النوع من السجلات يمكن للمحاكم أن تأخذ به، إذا كان برنامج الحاسوب يؤدي عمله على نحو جيد وسليم(22).

وبناءً على هذه القواعد، فإن الفقه في أمريكا يرى بأنه حتى يكون الدليل الرقمي مقبولاً أمام المحكمة، يجب أن يتوفر فيه الشروط التالية(23):

- أن لا يطرأ على محتويات السجل الإلكتروني أي تغيير، أي أن يكون الدليل المقدم إلى المحكمة هو نفس الدليل الذي تمّ جمعه، ويمكن للشخص الذي قام بجمع الدليل أن يشهد بذلك أمام

(21) الشهادة على السماع وفق قواعد الإثبات الفيدرالية تقبل على سبيل الاستثناء في المجالات التالية: الأعمال، المذاكرات اليومية، التقارير، السجلات، الأحداث، الشروط، الآراء، التشخيص. فإذا تمّ حفظ هذه الأشكال في الحاسوب بالأسلوب المعتاد ووفق نظام العمل السائد، فإنها تعد كالشهادة على السماع.
Albert .J. Mercella, op-cit, 22.
وأيضاً د.عمر بن يونس: الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، المرجع السابق، ص420-421.

(22) Albert .J. Mercella, op-cit, 23.
وأيضاً د.عمر بن يونس: الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، المرجع السابق، ص420-421.

(23) Eoghan casey,op-cit,p.78 .

المحكمة، وهذا ما يطلق عليه مفهوم "**سلسلة الرعاية**" Chain of Custody، ويقصد بذلك أن الدليل الرقمي منذ لحظة جمعه وحتى لحظة تقديمه إلى المحكمة لم يطرأ عليه أي تغيير، ولا يوجد أي احتمال للعبث به، وأنه تمّت مراعاة سلامته حتى يبقى بنفس الحالة التي وجد عليها[(24)].

- أن تكون المعلومات الموجودة في السجل، قد صدرت فعلاً عن المصدر المزعوم، سواء كان هذا المصدر الإنسان أم الآلة.
- أن تكون المعلومات الموجودة في السجل، والمتعلقة بالوقت والتاريخ، معلومات دقيقة.

أما القضاء الأمريكي فقد تعرض في العديد من القضايا إلى مسألتي الأصالة والصحة. ففي إحدى القضايا، قررت المحكمة: "إن عضو مكتب التحقيقات الفيدرالي FBI الذي كان حاضراً عندما تمّ ضبط الحاسوب الخاص بالمتهم، يمكن أن يقرر صحة الملفات المضبوطة."[(25)]. وفي قضية أخرى قبلت المحكمة سجلات الهاتف بعد أن أكّدت موظفة الفواتير في الشركة أصالة هذه السجلات[(26)]. كما قبلت إحدى المحاكم الدليل الرقمي رغم الدفوع المتعلقة بالعبث بهذا الدليل، لأن هذه الدفوع جاءت على شكل تخمين، دون أن يوجد أي دليل يدعمها[(27)]. وفي إحدى القضايا قررت المحكمة: "إن حقيقة وجود احتمال بتعديل البيانات الموجودة في الحاسوب غير كافية للقول بعدم جدارة الدليل."[(28)] كما ذكرت وزارة العدل الأمريكية في المرشد الفيدرالي لتفتيش وضبط الحواسيب، وصولاً إلى الدليل الإلكتروني في التحقيقات الجنائية: "إن غياب دليل واضح على حدوث العبث في الدليل، لا يؤثر على أصالة ودقة سجلات الحاسوب"[(29)].

---

(24) Dr. Henry B. wolfe, Forensics and the emerging importance of electronic Evidence gathering, OTAGO university, 2001, P-4, available on line. www.e-evidence.info. Albert .J. Mercella, op-cit, 343.

(25) Witaker, 127 F.3d 595, 601 (7th cir. 1997).
مشار إليه عند د.عمر بن يونس: الإجراءات الجنائية في القانون الأمريكي، المرجع السابق، ص 425.

(26) Eoghan casey,op-cit,p.170.

(27) Witaker, 127 F.3d at 602, Eoghan casey,op-cit,p.170.

(28) Bouallo, 858 F.2d 1427, 1436 (9th cir.1988). Eoghan casey, op-cit, p.170.

(29) Eoghan casey,op-cit,p.170.

ثانياً– إنكلترا:

في عام 1948 صدر في إنكلترا قانون الشرطة والإثبات الجنائي (Pace)[30]. وقد حدد هذا القانون الصلاحيات لشرطة "إنكلترا" و"ويلز"، وهو قانون يهدف إلى إقامة التوازن بين قوى الشرطة البريطانية وحقوق الأفراد، ويتناول آلية تفتيش الأماكن، وكيفية معاملة المشتبه بهم، والاعتقال وغير ذلك. وقد تم تعديل هذا القانون في 14 تشرين الأول عام 2002.

كما ركّز هذا القانون بصفة أساسية على قبول مخرجات الحاسوب كدليل في الإثبات، حيث حدد المشرع الإنكليزي في المادة 69 من هذا القانون الشروط الواجب توفرها في المستند الناتج عن الحاسوب، حتى يُقبل كدليل في الإثبات. وهذه الشروط هي[31]:

- عدم وجود أسس معقولة للاعتقاد بأن البيان يفقد الدقة بسبب الاستخدام غير المناسب أو الخاطئ للحاسوب.

- أن الحاسوب كان يعمل في جميع الأحوال بصورة سليمة، وإذا لم يكن كذلك، فإن أي جزء لم يكن يعمل فيه بصورة سليمة، أو كان معطلاً عن العمل، لم يكن ليؤثر في إخراج المستند أو دقة محتوياته.

وقد علق مجلس اللوردات على المادة 69 المشار إليها، بأنه: "يمكن للشهادة الشخصية الصادرة عن شخص على علم بطريقة تشغيل الحاسوب، أن تعطي الثقة بالدليل، وليس بالضروري أن يكون هذا الشخص خبيراً بالحاسوب"[32]. وبناءً على ذلك قبلت المحاكم الإنكليزية –فيما يتعلق بسلامة نظام الحاسوب– بشهادة أشخاص لديهم علم بطريقة عمل نظام الحاسوب[33].

ثالثاً– فرنسا:

يتناول الفقه في فرنسا حجية مخرجات الحاسوب في المواد الجنائية، في إطار مسألة أوسع وأعم، هي مسألة قبول الأدلة الناشئة عن الآلة أو الأدلة العلمية، مثل الرادارات، وأجهزة التصوير، وأشرطة

---

(30) وهو اختصار The Police Criminal Evidence Act ومتوفر على الإنترنت على موقع القوانين البريطانية www.briTishlaw.org.uk.

(31) فهد سلطان محمد أحمد بن سليمان: المرجع السابق، ص146. د. هلالي عبد اللاه أحمد: المرجع السابق، ص53. د. عمر بن يونس: الجرائم الناشئة عن استخدام الإنترنت،المرجع السابق، ص993.

(32) Eoghan casey,op-cit,p.170

(33) R.V Shephard. 1933, Eoghan casey,op-cit,p.170.

التسجيل، وأجهزة التنصت.

أما القضاء فقد قبل هذه الأدلة إذا توفرت فيها مجموعة من الشروط، من أهمها أن يتم الحصول عليها بطريقة شرعية ونزيهة، وأن يتم مناقشتها حضورياً من قبل الأطراف. وقد قضت محكمة النقض الفرنسية بأن أشرطة التسجيل الممغنطة، التي يكون لها قيمة دلائل الإثبات، يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي(34).

أما بالنسبة إلى قناعة القاضي الجزائي، فإن الأدلة الإلكترونية تخضع لحرية القاضي في الاقتناع الذاتي، بحيث يمكن أن يطرح مثل هذه الأدلة – رغم قطعيتها من الناحية العلمية– عندما يجد أن الدليل الإلكتروني لا يتسق منطقياً مع ظروف الواقعة وملابساتها(35).

رابعاً– المنظمة الدولية لدليل الحاسوب:

تأسست المنظمة الدولية لدليل الحاسوب IOCE (36) في عام 1995، وتتكون من الجهات الحكومية المسؤولة عن تطبيق القانون، أو من الهيئات الحكومية التي تزاول التحقيق في مجال الحاسوب. وتهدف هذه المنظمة إلى تزويد الجهات الدولية القانونية بكيفية تبادل المعلومات بتحقيقات جرائم الحاسوب والمسائل ذات الصلة بالمعلوماتية الشرعية. كما تقوم بتنظيم عملية الاتصال بين أعضائها، وتقدم التوصيات اللازمة في هذا المجال، وتقيم المؤتمرات المتعلقة بنشاطاتها.

وإضافةً إلى ذلك فإن المنظمة وضعت المعايير المطلوبة في دليل الحاسوب، وقد تمت المصادقة على هذه المعايير خلال المؤتمر الدولي للبحث المعلوماتي والجريمة التقنية، المنعقد في تشرين الأول عام 1999 (IHCFC)(37)، وهذه المعايير هي(38):

- عدم تغير الدليل أثناء ضبطه.
- أن تتم عملية الضبط من قبل شخص مؤهلٍ في المعلوماتية الشرعية.

---

(34) Cass. Criw. 28 avr. 1987, Bull. Criw.no.173

مشار إليه عند: د. هلالي عبد اللاه أحمد: المرجع السابق، ص43. د. علاء عبد الباسط خلاف: المرجع السابق، ص450.

(35) علي حسن محمد الطوالبة: المرجع السابق، ص191.

(36) وهو اختصار لـInternational Organization on computer Evidence.

(37) وهو اختصار لـInternational Hi- tech crime and Forensics conference.

(38) ALBERT. J. Marcella, op- cit, p.141. And available on www.Ioce.org.

- جميع النشاطات المتعلقة بالضبط والوصول والتخزين ونقل الدليل الرقمي، يجب أن تكون موثقة ومحفوظة بغرض التدقيق.
- أن يكون الشخص الذي بحوزته الدليل الرقمي مسؤولاً عن جميع الإجراءات المتعلقة بهذا الدليل.
- أن تكون الجهات المسؤولة عن ضبط وتخزين ونقل الدليل الرقمي والوصول إليه مسؤولة عن تطبيق هذه المبادئ.

خامساً- سورية:

نصت المادة 25 من قانون مكافحة الجريمة المعلوماتية على ما يلي :

(أ- يعود للمحكمة تقدير قيمة الدليل الرقمي، شريطة تحقُّق ما يلي:

1) أن تكون الأجهزة الحاسوبية أو المنظومات المعلوماتية المستمدّ منها هذا الدليل تعمل على نحو سليم.

2) ألاّ يطرأ على الدليل المقدَّم إلى المحكمة أي تغيير خلال مدة حفظه.

ب - يعدّ الدليل الرقمي المقدَّم إلى المحكمة مستجمعاً للشرطين الواردين في الفقرة (أ) من هذه المادة، ما لم يثبت العكس.)

يستمد القاضي الجزائي قناعته من أي دليل يطمئن إليه من الأدلة التي تقدم في الدعوى دون التقيد بدليل معين، ما لم ينص القانون على غير ذلك؛ فلا يوجد أدلة يحظر القانون عليه قبولها. فالقانون أمدّ القاضي الجزائي بسلطة واسعة وحرية كاملة في مجال الإثبات، فله أن يأخذ من الأدلة ما تطمئن له عقيدته، ويطرح ما لا يرتاح إليه. وهذا ما نصت عليه الفقرة الأولى من المادة 175 من قانون أصول المحاكمات الجزائية بقولها: (تقام البينة في الجنايات والجنح والمخالفات بجميع طرق الإثبات، ويحكم القاضي حسب قناعته الشخصية).

و الدليل الرقمي يندرج تحت طائفة **القرائن القضائية** إذا تم الحصول عليه **بطريقة مشروعة،** ويمكن للقاضي الجزائي الأخذ به سواء في إطار الإدانة أم البراءة، **إذا توفرت في هذا الدليل الشرطين التاليين:**

1- **السلامة:** أي أن تكون الأجهزة الحاسوبية أو المنظومات المعلوماتية المستمدّ منها هذا الدليل تعمل على نحو سليم، بحيث لا يتطرق الشك في دقته.

2- **المطابقة:** أن لا يطرأ على هذا الدليل أي تغيير خلال فترة حفظه، أي أن يكون الدليل الرقمي المقدم إلى المحكمة هو نفس الدليل الذي تم جمعه وحفظه.

وقد وضع المشرع **قرينة قانونية بسيطة** في الفقرة (ب) من المادة 25، تتضمن أن الدليل الرقمي المقدَّم إلى المحكمة يعدّ مستجمعاً لشرطّي السلامة والمطابقة المشار إليهما ما لم يثبت العكس.

أما بالنسبة إلى **الدفوع** المتعلقة بهذين الشرطّين، فإن هذه الدفوع يجب أن لا تنال من قيمة الدليل الرقمي إذا جاءت على شكل تخمين دون أن يوجد دليل يدعمها. وهذا ما سارت عليه المحاكم الأمريكية كما رأينا.

وفيما يتعلق **بكيفية تقدير قيمة الدليل الرقمي،** فإننا **نؤيد** ما ذهب إليه جانب من الفقه العربي من ضرورة التمييز بين أمرين، هما:

الأمر الأول: القيمة العلمية القاطعة للدليل.

الأمر الثاني: الظروف والملابسات التي وجد فيها الدليل.

فتقدير القاضي لا يتناول القيمة العلمية القاطعة للدليل، ذلك لأن قيمة الدليل تقوم على أسس علمية دقيقة، ولا حرية للقاضي في مناقشة الحقائق العلمية الثابتة. أما ما يتعلق بالظروف والملابسات التي وجد فيها هذا الدليل، فإنها تدخل في نطاق تقديره الشخصي لأنها من طبيعة عمله، ومن ثم فللقاضي الجزائي أن يطرح الدليل المستخرج من الحاسوب عندما يجد أن وجوده لا يتفق منطقياً مع ظروف الواقعة. فمجرد توفر الدليل العلمي لا يعني أن يحكم القاضي مباشرة دون البحث بالظروف والملابسات[39].

وبعد أن انتهينا من دراسة فصل الأحكام الإجرائية للجريمة المعلوماتية، لا بد لنا من الإشارة بأن المادة 35 من قانون مكافحة الجريمة المعلوماتية، قضت بأن يُطبَّق قانون أصول المحاكمات الجزائية النافذ على كل ما لم يردّ عليه نصّ في الأحكام الإجرائية للجرائم الواردة في قانون مكافحة الجريمة المعلوماتية.

---

(39) د.هلالي عبد اللاه أحمد: المرجع السابق، ص46 و47 د. جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2002، ص22. د.علي جبار الحسيناوي: المرجع السابق، ص142. علي حسن محمد الطوالبة: المرجع السابق، ص178. د. علاء عبد الباسط خلاف: المرجع السابق، ص451.

وأخيراً بعد أن انتهينا من دراسة جرائم المعلوماتية من الناحية الموضوعية و الناحية الإجرائية، أرجو الله أن أكون قد عرضت الموضوع عرضاً شاملاً وافياً بالغرض، وأن أكون قد وُفقت في شرحه، فإن أصبت فلله المنّة والفضل، وإن أخطأت فالعصمة من شأن الرسل.

تمارين:

اختر الإجابة الصحيحة: بالنسبة للدليل الرقمي:

1. لم ينص قانون مكافحة الجريمة المعلوماتية على حجيته.
2. يشترط في الدليل الرقمي شرطي السلامة والمطابقة.
3. وضع المشرع بالنسبة لحجية الدليل الرقمي قرينة قانونية قاطعة.
4. لا يمكن للقاضي تقدير الظروف والملابسات التي تم فيها الحصول على الدليل.

الإجابة الصحيحة رقم 2

((المـــراجع))

أولاً – المراجع باللغة العربية:

أ- المراجع العامة :

– **د.حسن الجوخدار:** أصول المحاكمات الجزائية، الطبعة الخامسة، منشورات جامعة دمشق، 1991.

– **العلامة رينيه غارو:** موسوعة قانون العقوبات العام والخاص، عشر مجلدات، منشورات الحلبي الحقوقية، بيروت،ترجمة المحامية لين صلاح مطر ، 2003.

– **د.عبد الوهاب حومد:**

- أصول المحاكمات الجزائية، الطبعة الرابعة (منقحة ومزيدة)، المطبعة الجديدة، دمشق، 1987.
- المفصّل في شرح قانون العقوبات، القسم العام، المطبعة الجديدة، دمشق، 1990.

– **د.عبود السراج،** شرح قانون العقوبات، القسم العام، منشورات جامعة دمشق، 2007 .

– **د.علي عبد القادر القهوجي:** قانون العقوبات – القسم الخاص، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2001.

– **د.محمود نجيب حسني:**

- شرح قانون العقوبات اللبناني – القسم العام، المجلد الأول، الطبعة الثالثة (معدلة ومنقحة)، منشورات الحلبي الحقوقية، بيروت، عام 1988.
- شرح الجرائم الواقعة على الأموال في قانون العقوبات اللبناني (جزأن)، طبعة ثالثة جديدة (معدلة و منقحة)، منشورات الحلبي الحقوقية، بيروت، 1998 .
- شرح قانون الإجراءات الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة، 1988.

ب – المراجع المتخصصة :

– **د. الشحات إبراهيم محمد منصور**، الجرائم الالكترونية في الشريعة الإسلامية و القوانين الوضعية، دار النهضة العربية، القاهرة، 2002 .

– **القاضي الدكتور إيهاب السنباطي:** موسوعة الإطار القانوني للتجارة الالكترونية، دار النهضة العربية، القاهرة، 2007.

– **د.جميل عبد الباقي الصغير:**

- الإنترنت و القانون الجنائي، دار النهضة العربية، القاهرة، 2002.
- أدلة الإثبات الجنائي و التكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2002 .
- الحماية الجنائية والمدنية لبطاقات الائتمان، دار النهضة العربية، القاهرة، 2003 .
- الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 2002 .

– **د.حسين بن سعيد الغافري**، السياسة الجنائية في مواجهة جرائم الإنترنت(دراسة مقارنة)، دار النهضة العربية، القاهرة،2009.

– **د.سليمان أحمد فضل:** المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، 2007.

– **د.طوني ميشال عيسى:** التنظيم القانوني لشبكة الإنترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2001.

– **عبد الله عبد الكريم عبد الله:** جرائم المعلوماتية والإنترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2007.

– **د.عبد الفتاح بيومي حجازي:**

- التجارة الالكترونية وحمايتها القانونية، دار الفكر الجامعي، الإسكندرية، 2004.
- مبادئ الإجراءات الجنائية، في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، المحلة الكبرى، القاهرة، 2007.

– **د.عبد الفتاح مراد:** شرح جرائم الكمبيوتر والإنترنت، بلا دار نشر، بلا عام.

– **د.علاء عبد الباسط خلاف:** الحماية الجنائية لوسائل الاتصال الحديثة، دار النهضة العربية، القاهرة، 2002.

– **د.علي جبار الحسيناوي:** جرائم الحاسوب والإنترنت، الطبعة العربية، دار اليازوري العلمية للنشر والتوزيع، عمان، 2009.

– **د.عمر محمد أبو بكر بن يونس :**

- الجرائم الناشئة عن استخدام الإنترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، 2004 .

- الإجراءات الجنائية عبر الإنترنت في القانون الأمريكي، الطبعة الأولى، بدون اسم الناشر، القاهرة، 2005 .
- الاتفاقية الأوربية حول الجريمة الافتراضية (المذكرة التفسيرية)، الطبعة الثانية، مؤسسة آدم للنشر والتوزيع، مالطا، 2008.

–**القاضي الدكتور غسان رباح:** الوجيز في قضايا حماية الملكية الفكرية والفنية مع دراسة مقارنة حول جرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2008.

– **المحامي محمد أمين الشوابكة:** جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2006.

– **د.محمد الشناوي:** جرائم النصب المستحدثة، دار الكتب القانونية، المحلة الكبرى، القاهرة، 2008.

– **د. مصطفى محمد موسى:** دليل التحري عبر شبكة الإنترنت، دار الكتب القانونية، القاهرة، 2005.

– **المحاميان منير محمد الجنبيهى وممدوح محمد الجنبيهى:**جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2005.

– **د.نائلة عادل محمد فريد قورة:** جرائم الحاسوب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2005.

– **نبيلة هبة هروال**،الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2007 .

– **د.هدى حامد قشقوش:** جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، بلا عام.

– **د. هلالي عبد اللاه أحمد :** حجية المخرجات الكومبيوترية في المواد الجنائية، النسر الذهبي للطباعة، القاهرة، 2002 .

– **وائل الدبيسي:** البطاقة المصرفية، مطبعة صادر، بيروت، 2004.

ج- رسائل الماجستير والدكتوراه :

– **أحمد حسام طه تمام:** الجرائم الناشئة عن استخدام الحاسب الآلي، دراسة مقارنة، رسالة دكتوراه مقدمة لجامعة طنطا، 2000.

– **علي حسن محمد طوالبة:** التفتيش الجنائي على نظم الحاسوب والإنترنت، رسالة لنيل درجة الدكتوراه مقدمة إلى جامعة عمان العربية للدراسات العليا، 2003.

– فهد سلطان محمد أحمد بن سليمان، مواجهة جرائم الإنترنت، رسالة حاصلة على درجة الماجستير في القانون الجنائي بجامعة القاهرة 2002.

– **د.محمد سعيد أحمد إسماعيل:** أساليب الحماية القانونية لمعاملات التجارة الإلكترونية، رسالة دكتوراه مقدمة من جامعة عين شمس، القاهرة، 2005.

- **محمد عبيد الكعبي:** الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت، رسالة حاصلة على درجة الماجستير في القانون الجنائي بجامعة القاهرة، 2004 .

د- الأبحاث:

- **د.علي محمود علي حمودة:** الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية المنعقد في دبي من 26 – 28 نيسان، 2003. متوفر على الموقع www.arablawinfo.com .

هـ - الدوريات:

- **د. مصطفى محمد موسى:** المراقبة الإلكترونية عبر شبكة الإنترنت، دراسة مقارنة، سلسلة اللواء الأمنية في مكافحة الجريمة الإلكترونية، العدد الخامس، مطابع الشرطة للطباعة والنشر والتوزيع، القاهرة، 2003.

و- القواميس التقنية:

- **د.عبد الحسن الحسيني:** القاموس الموسوعي في المعلومات والاتصالات والمعلوماتية القانونية، الطبعة الأولى، مكتبة صادر، بيروت، 2004.

ز- مجموعات الاجتهادات القضائية:

- مجموعة أحكام النقض في قانون العقوبات والقوانين المتممة من عام 1988 حتى 2001، إعداد عبد القادر جار الله، الطبعة الأولى، المكتبة القانونية، دمشق، 2001.

<u>ثانياً – المراجع باللغة الأجنبية :</u>

1) **Adam D Thierer**، Clyed wayne crews، Who rules the net?، published by cat to institute، 2003، ISBN: 9781930865433 .

2) **ALBERT .J . Marcella**، **Robert .s. Green Field**، Cyber Forensics، Field Manual for collecting Examining and Preserving Evidence of computer crimes، published by CRC Press، 2002، ISBN:9780849309557.

3) **Allen Hammond**، Santa Clara University، The 2001 Council Of Europe Convention On Cyber- Crime An efficient Tool To Fight Crime On Cyber-space، 2001.

4) **Anthony Reys and others**، Cyber Crime Investigations، Bridging The Gaps Between Security Professional Law، Enforcement and Prosecutors. Published by Elsevier Since and Technology، 2007، ISBN: 9781597491334.

5) **Charles Doyle**: Cyber Crime: An Overview Of The Fraud Computer Fraud and Abuse Statute، 2008.

6) **Eoghn Casey**: Digital Evidence And Computer Crime، second edition، A cadimic Press، 2004. ISBN، 0121631044.

7) **Dr. Henry B. wolfe**، Forensics and the emerging importance of electronic Evidence gathering، OTAGO university، 2001، available on line. www.e-evidence.info.

8) **Joseph T. wells**: Computer Fraud Casebook، Published by John Wiely @sons. Inc، Hoboken، New Jersey، 2009، ISBN: 9780470278147.

9) **Micheal Hirst**، Jurisdiction and the Ambit of the criminal law، published by oxford university، 2003، ISBN: 9780199245390.

10) **Micheal Kunz and Patrick Wilson**: computer crime and computer fraud، University of Mayland، 2004.

11) On line fraud and crime: Are consumers safe? Hearing before the subcommittee on commerce trade and consumer protection، 2001.

12) **Richard Hillman**: securities fraud، The internet poses challenges to

Regulateres and Investors، United States General Accounting Office، 1999.

13) **Robin Bryant**: Investigating Digital Crime، John Wile& Sons، ltd، 2008، ISBN: 9780470516003 .

14) **Report**: internet crime compliment center، 2007. Available on www.ic3.gov